PUBLIC

SAP BusinessObjects Business Intelligence platform

Document Version: 2025 – 2025-03-12

Business Intelligence Platform Administrator Guide

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

Content

1 Document History. 19

2 Getting Started. 20

2.1 About this guide. 20

Who should use this guide?. 20

About the Business Intelligence platform. 20

Variables. 21

Terminology. 21

2.2 Before you start. 23

Key concepts. 23

Key administrative tools. 25

Key tasks. 28

3 Architecture. 31

3.1 Architecture overview. 31

Component diagram. 32

Architecture tiers. 32

Databases. 34

Servers, hosts, and clusters. 35

Web application servers. 35

Software Development Kits. 39

Data sources. 41

Authentication and single sign-on. 42

SAP Integration. 43

Integrated version control. 44

3.2 Servers, services, nodes, and hosts. 44

Server changes since XI 3.1. 46

Services. 48

Service categories. 53

Server types. 55

Servers. 57

3.3 Client applications. 58

Installed with SAP BusinessObjects Business Intelligence platform Client Tools. 59

Installed with SAP BusinessObjects Business Intelligence platform. 61

Available separately. 62

Web application clients. 63

3.4 Process Workflows. 65

Startup and authentication. 65
Program objects. 67
Crystal Reports. 69
Web Intelligence. 73

4 System Configuration Wizard. 76
4.1 Introduction to the System Configuration Wizard. 76
4.2 Specifying the products you use. 76
4.3 Choosing a deployment template. 78
4.4 Specifying data folder locations. 79
4.5 Reviewing your changes. 81
4.6 Log files and response files. 81
Using a response file. 82

5 Managing Licenses. 85
5.1 Managing license keys. 85
To view license information. 85
To add a license key. 86
To view current account activity. 87

6 Managing Users and Groups. 88
6.1 Account management overview. 88
User management. 88
Group management. 88
Available authentication types 89
6.2 Managing Enterprise and general accounts. 90
To create a user account. 90
To modify a user account. 91
To delete a user account. 92
To create a new group. 93
To modify a group's properties. 93
To view group members. 94
To add subgroups. 95
To specify group membership. 95
To delete a group. 96
To add users or user groups in bulk. 97
To enable the Guest account. 98
Adding users to groups. 98
Changing password settings. 100
Granting access to users and groups. 102
Controlling access to user inboxes. 102
Configuring Fiorified BI launch pad options. 103

Managing attributes for system users . . . 106
Prioritizing user attributes across multiple authentication options. . . . 107
To add a new user attribute. . . . 108
To edit customized user attributes. . . . 109
6.3 Managing aliases. . . . 110
To create a user and add a third-party alias. . . . 110
To create a new alias for an existing user. . . . 111
To assign an alias from another user. . . . 112
To delete an alias. . . . 113
To disable an alias. . . . 113

7 Setting Rights. . . . 115
7.1 How rights work in BI platform. . . . 115
Access levels. . . . 115
Advanced rights settings. . . . 116
Inheritance. . . . 117
Type-specific rights. . . . 121
Determining effective rights. . . . 123
7.2 Managing security settings for objects in the CMC. . . . 123
To view rights for a principal on an object. . . . 124
To assign principals to an access control list for an object. . . . 125
To modify security for a principal on an object. . . . 125
To set rights on a top-level folder in the BI platform. . . . 126
Checking security settings for a principal. . . . 127
7.3 Working with access levels. . . . 129
Choosing between *View* and *View On Demand* access levels. . . . 131
To copy an existing access level. . . . 132
To create a new access level. . . . 132
To rename an access level. . . . 133
To delete an access level. . . . 133
To modify rights in an access level. . . . 133
Tracing the relationship between access levels and objects. . . . 134
Managing access levels across sites. . . . 135
7.4 Breaking inheritance. . . . 136
To disable inheritance. . . . 137
7.5 Using rights to delegate administration. . . . 138
Choosing between "*Modify the rights users have to objects*" options. . . . 139
Owner rights. . . . 140
7.6 Summary of recommendations for rights administration. . . . 141

8 Securing the BI Platform. . . . 142
8.1 Security overview . . . 142

8.2 Secure use of program objects. . . . 142
8.3 Disaster recovery planning. . . . 143
8.4 General recommendations for securing your deployment. . . . 143
8.5 Configuring security for bundled third-party servers. . . . 145
8.6 Authentication. . . . 145
Active trust relationship. . . . 145
Trusted Authentication. . . . 146
8.7 Sessions and session tracking. . . . 147
CMS session tracking. . . . 148
Managing sessions. . . . 148
Script to clear Stale Sessions. . . . 150
8.8 Environment protection. . . . 150
Web browser to web server. . . . 151
Web server to BI platform. . . . 151
Protection against malicious logon attempts. . . . 151
Password restrictions. . . . 151
Logon restrictions. . . . 152
User restrictions. . . . 152
Guest account restrictions. . . . 152
8.9 Auditing security configuration modifications 153
8.10 Processing extensions. . . . 153
8.11 Virus Scan Interface. . . . 153
Enabling Virus Scan. . . . 154
8.12 BI platform data security. . . . 155
Data processing security modes. . . . 155
Administrator accounts. . . . 158
Connection rights. . . . 158
8.13 Cryptography in the BI platform. . . . 159
Working with cluster keys. . . . 160
Cryptographic Officers. . . . 162
Managing cryptographic keys in the CMC. . . . 164
8.14 Data Protection and Privacy. . . . 169
Glossary. . . . 170
User Consent. . . . 171
Information Report. . . . 171
Read Access Logging. . . . 172
Deletion of Personal Data. . . . 172
Change Log. . . . 173
8.15 Configuring backend servers for SSL. . . . 174
To create the default configuration file. . . . 175
Creating key and certificate files. . . . 176

Setting up SSL when the certificate is managed by a certificate authority. 178
Configuring the SSL protocol. 180
8.16 Understanding communication between BI platform components. 185
Overview of BI platform servers and communication ports. 186
Communication between BI platform components 188
8.17 Configuring the BI platform for firewalls. 196
To configure the system for firewalls. 197
Debugging a firewalled deployment. 200
8.18 Examples of typical firewall scenarios. 201
Example - Application tier deployed on a separate network. 202
Example - Thick client and database tier separated from BI platform servers by a firewall. 204
8.19 Firewall settings for integrated environments. 206
Specific firewall guidelines for SAP integration. 207
Firewall configuration for JD Edwards EnterpriseOne integration. 208
Specific firewall guidelines for Oracle EBS. 210
Firewall configuration for PeopleSoft Enterprise integration 210
Firewall configuration for Siebel integration. 212
8.20 The BI platform and reverse proxy servers 213
Understanding how web applications are deployed 213
8.21 Configuring reverse proxy servers for BI platform web applications. 214
Detailed instructions for configuring reverse proxy servers. 214
To configure the reverse proxy server. 215
To configure Apache 2.2 reverse proxy server for the BI platform 215
To configure WebSEAL 6.0 reverse proxy server for the BI platform 216
To configure Microsoft ISA 2006 for the BI platform 217
8.22 Special configuration for the BI platform in reverse proxy deployments. 219
Enabling reverse proxy for web services. 219
Enabling the root path for session cookies for ISA 2006. 222
Enabling reverse proxy for SAP BusinessObjects Live Office. 224

9 Authentication. 226
9.1 Authentication options in the BI platform. 226
Primary authentication. 226
Security plug-ins. 227
Single sign-on to the BI platform. 228
9.2 Enterprise authentication. 231
Enterprise authentication overview. 231
Enterprise authentication settings. 231
To change Enterprise settings. 232
SAML 2.0 Authentication. 234
Enabling Trusted Authentication. 243
Configuring Trusted Authentication for the Web Application. 250

9.3 LDAP authentication. . . . 259
Using LDAP authentication. . . . 259
Configuring LDAP authentication. . . . 261
Mapping LDAP groups. . . . 272
9.4 Windows AD authentication. . . . 284
Using Windows AD authentication. . . . 284
Preparing the Domain Controller. . . . 285
Configuring AD Authentication in the CMC. . . . 286
Configuring the BI platform service to run the SIA. . . . 294
Configuring the web application server for AD Authentication. . . . 297
Single Sign-On Setup. . . . 303
Troubleshooting Windows AD authentication. . . . 321
9.5 SAP authentication. . . . 322
Configuring SAP authentication 322
Creating a user account for the BI platform. . . . 323
Connecting to SAP entitlement systems. . . . 325
Setting SAP Authentication options. . . . 327
Importing SAP roles. . . . 331
Configuring Secure Network Communication (SNC). . . . 335
Setting up single sign-on to the SAP system. . . . 349
Configuring SSO for SAP Crystal Reports and SAP NetWeaver. . . . 354
9.6 PeopleSoft authentication. . . . 356
Overview. . . . 356
Enabling PeopleSoft Enterprise authentication. . . . 356
Mapping PeopleSoft roles to the BI Platform. . . . 357
Scheduling user updates. . . . 360
Using the PeopleSoft Security Bridge. . . . 361
9.7 X.509 Authentication. . . . 370
X.509 Authentication for BI Launch Pad. . . . 370
X.509 Authentication for Web Services. . . . 380
X.509 Authentication for CMC. . . . 384
9.8 OpenID Connect authentication. . . . 387
Enabling OpenID Connect authentication. . . . 388

10 Data Source Reference. . . . 389
10.1 Enhanced Credential Mapping. . . . 389
Create a data source reference. . . . 390
Define the database credentials against a data source reference for a user in CMC. . . . 391
Define the database credentials against a data source reference for a user in BI Launch Pad 392
Define the database credentials against a data source reference for a group. . . . 393
Associate data source reference in OLAP connection. . . . 394

Secondary Credentials — Key Rotation Administration. 394

11 Server Administration. 402

11.1 Working with the Servers management area in the CMC. 402

11.2 Managing servers by using scripts on Windows 405

11.3 Managing servers on Unix 405

11.4 Viewing and changing a server's status. 405

Viewing the state of servers. 405

Starting, stopping, and restarting servers. 407

Stopping a Central Management Server. 409

Enabling and disabling servers. 410

11.5 Adding, cloning, or deleting servers. 411

Adding, cloning, and deleting servers. 411

11.6 Add Custom Internet Headers. 414

11.7 Clustering Central Management Servers. 416

Clustering Central Management Servers. 416

11.8 Managing server groups. 420

Creating a server group. 420

Converting an exclusive server group to non-exclusive and vice-versa. 423

Working with server subgroups. 424

Modifying the group membership of a server. 426

Administrative access to servers and server groups for users. 427

Mapping a User Group to a Server Group. 429

Mapping a Folder to a Server Group. 432

Understanding Server Group Rights Management. 434

11.9 Configuring Adaptive Processing Servers for production systems. 438

11.10 Assessing your system's performance. 439

Monitoring BI platform servers. 439

Analyzing server metrics. 439

Viewing system metrics. 440

Logging server activity. 440

11.11 Configuring server settings. 441

To change a server's properties. 442

To apply service settings to multiple servers. 442

Working with configuration templates. 443

11.12 Configuring server network settings. 446

Network environment options. 446

Server host identification options. 447

Configuring a multi-homed machine. 449

Configuring port numbers. 451

11.13 Managing Nodes. 455

Using nodes. 455

Adding a new node. . . . 457
Recreating a node. . . . 462
Deleting a node. . . . 466
Renaming a node. . . . 469
Moving a node. . . . 471
Script parameters. . . . 475
Adding Windows server dependencies. . . . 479
Changing the user credentials for a node. . . . 480
11.14 Renaming a machine in a BI platform deployment. . . . 481
Changing cluster names. . . . 481
Changing IP addresses. . . . 481
Renaming machines. . . . 483
11.15 Using 32-bit and 64-bit third-party libraries with BI platform. . . . 485
11.16 Managing server and node placeholders. . . . 486
To view server placeholders. . . . 486
To view and edit the placeholders for a node. . . . 487

12 Managing Central Management Server (CMS) Databases. . . . 488
12.1 Managing CMS system database connections. . . . 488
To select SQL Anywhere as a CMS database. . . . 488
To select SAP HANA as a CMS database. . . . 489
12.2 Selecting a new or existing CMS database. . . . 490
To select a new or existing CMS database on Windows. . . . 492
To select a new or existing CMS database on UNIX. . . . 492
12.3 Recreating the CMS system database. . . . 493
To recreate the CMS system database on Windows. . . . 493
To recreate the CMS system database on UNIX. . . . 494
12.4 Copying data from one CMS system database to another. . . . 495
Preparing to copy a CMS system database. . . . 496
To copy a CMS system database on Windows. . . . 496
To copy data from a CMS system database on UNIX. . . . 497
12.5 Central Management Server Database Driver. . . . 498

13 Backing Up and Restoring Your System. . . . 499
13.1 Overview of backup and restore. . . . 499
13.2 Terminology. . . . 499
13.3 Use cases for backup and restore. . . . 500
13.4 Backups. . . . 502
Backing up the entire system. . . . 502
Backing up server settings. . . . 506
Backing up BI content. . . . 509
13.5 Restoring your system. . . . 509

Restoring your entire system. . . . 510
Restoring server settings. . . . 517
Restoring BI content. . . . 521
13.6 BackupCluster and RestoreCluster scripts. . . . 521

14 Copying Your BI Platform Deployment. . . . 524
14.1 Overview of system copying. . . . 524
14.2 Terminology. . . . 524
14.3 Use cases for system copying. . . . 524
14.4 Planning to copy your system. . . . 525
14.5 Considerations and limitations. . . . 526
14.6 System copy procedure. . . . 528
To export from a source system. . . . 528
To import to a target system. . . . 532

15 Promotion Management. . . . 535
15.1 Welcome to promotion management. . . . 535
Overview. . . . 535
Features. . . . 535
Application access rights. . . . 536
Support for WinAD in promotion management. . . . 537
15.2 Getting started with the promotion management tool. . . . 537
Accessing the promotion management tool. . . . 537
User interface components. . . . 538
Using the Settings option. . . . 540
15.3 Using the promotion management tool. . . . 546
Creating and deleting folders. . . . 547
To create a job. . . . 548
To create a new job by copying an existing job 551
To search for a job. . . . 551
To edit a job. . . . 552
To add an infoobject to a job. . . . 553
To manage the dependencies of a job. . . . 554
To search for dependents 555
To promote a job when repositories are connected. . . . 556
Promoting a job using an LCMBIAR File. . . . 559
To schedule a job promotion. . . . 563
To view the history of a job. . . . 565
To roll back a job. . . . 565
15.4 Promoting full repository content using the promotion management tool. . . . 568
To prepare the source and target systems. . . . 568
Migration strategies. . . . 570

15.5 Full system promotion steps. . . . 571
To promote users and user groups (Job 1). . . . 572
To promote dependent objects (Job 2). . . . 572
To promote primary objects (Job 3). . . . 574
Post-promotion. . . . 575
15.6 Using the Command Line option. . . . 575
To run the command-line tool on Windows. . . . 576
To run the command-line tool on Unix. . . . 576
Command-line tool parameters. . . . 577
Sample properties file. . . . 600
15.7 Using the Promotion Management Wizard 601
To exclude objects from promotion. . . . 602
When to use the Promotion Management Wizard. . . . 603
Scenario. . . . 604
Objects. . . . 606
Dependencies. . . . 611
Summary. . . . 611
(optional) Properties file. . . . 612
Promotion Management Wizard on Linux. . . . 616

16 Version Management. . . . 617
16.1 To manage different versions of an infoobject. . . . 617
Version Management application access rights. . . . 618
16.2 To manage different versions of BI resources 618
16.3 To use Git as the Version Management System. . . . 620
16.4 To compare different versions of the same job. . . . 621

17 Managing Applications. . . . 623
17.1 Disabling the GDPR Popup Message. . . . 623
17.2 Managing applications through the CMC. . . . 625
Overview. . . . 625
Common settings for applications. . . . 626
Application-specific settings. . . . 627
17.3 Managing applications through Semantic Layer Properties. . . . 675
17.4 Managing applications through BOE.war properties. . . . 676
The BOE war file. . . . 676
17.5 Customizing BI launch pad and OpenDocument logon entry points. . . . 692
BI launch pad and OpenDocument file locations. . . . 692
To define a custom logon page. . . . 693
To add trusted authentication at logon. . . . 694
17.6 Customizing application user interfaces. . . . 695
Web Intelligence. . . . 695

BI launch pad. . . . 702
17.7 Configuring BI Platform RESTful Web Services on Web Server. . . . 702

18 Managing Connections and Universes. . . . 706
18.1 Managing connections. . . . 706
To delete a universe connection. . . . 707
OLAP data source connections. . . . 707
18.2 Managing universes. . . . 720
To delete universes. . . . 721

19 BI Admin Studio. . . . 722
19.1 Admin Cockpit. . . . 723
Admin Cockpit. . . . 723
BI on Servers. . . . 724
BI on Document Instances. . . . 725
BI on Users and Sessions. . . . 725
BI on Content Usage. . . . 726
BI on Applications. . . . 727
19.2 Monitoring. . . . 727
Monitoring terms. . . . 728
Configuring database support for Monitoring 731
Configuration properties. . . . 740
Integrating with other applications. . . . 747
Cluster support for monitoring server. . . . 747
Troubleshooting. . . . 748
19.3 Visual Difference. . . . 751
To compare objects or files using Visual Difference. . . . 751
To compare objects or files using the Version Management System. . . . 753
19.4 Authorizing HTML elements. . . . 753
To modify the list of authorized HTML elements. . . . 756

20 CMS Reporting. . . . 757
20.1 CMS Reporting. . . . 757
The architecture of the SAP BusinessObjects platform. . . . 757
The structure of the CMS system database. . . . 758
About InfoObjects. . . . 760
20.2 Overview of CMS reporting. . . . 762
20.3 CMS database connection. . . . 763
20.4 CMS reporting sample kit. . . . 764
Importing the CMS reporting sample kit with Promotion Management. . . . 765
The CMS sample universe 766
Extending the CMS sample universe. . . . 766

20.5 Creating a report on CMS. 767

21 Workflow Assistant. 768
21.1 Target Audience. 769
21.2 Understanding the Architecture. 770
21.3 Glossary. 771
21.4 About Installation and Update. 773
21.5 Configuring the Workflow Assistant. 774
Basic Configuration. 774
21.6 Managing Workflow Assistant Rights Via the Central Management Console. 777
21.7 Working with the Workflow Assistant. 782
About Standard Task Templates. 782
About Standard Workflow Templates. 791
About Custom Task Templates. 792
Managing Workflow Templates. 793
Managing Scenarios and Viewing Results. 795
Understanding the States of Task Templates, Workflow Templates and Scenarios. 801
Working with Systems. 802
End-to-End Process Flow of the Workflow Assistant. 806
21.8 Checking Log Files. 806

22 Recycle Bin. 808
22.1 Recycle Bin. 808
Restoring an Item from the Recycle Bin. 809
Permanently Deleting Items from the Recycle Bin. 810
Enabling Auto-Cleanup for the Recycle Bin. 810

23 Auditing. 812
23.1 Overview. 812
23.2 CMC Auditing page. 818
Auditing Status. 818
Configuring Auditing events. 820
Auditing Data Store Configuration Settings. 824
23.3 Audit events. 826
Audit events and details. 835

24 Events. 855
24.1 About Events. 855
User Notifications. 856

25 Platform Search. 861
25.1 Understanding Platform Search. 861
Platform Search SDK. 861

Clustered Environment. . . . 861
25.2 Setting Up Platform Search. . . . 862
Deploying OpenSearch. . . . 862
Configuring reverse proxy. . . . 864
Configuring Application Properties in the CMC. . . . 865
25.3 Working with Platform Search. . . . 871
Indexing Content in the CMS Repository. . . . 871
Indexing Failure Listing. . . . 872
Searching Results. . . . 873
25.4 Auditing. . . . 879
25.5 Troubleshooting. . . . 880
Self Healing. . . . 880
Problem Scenarios. . . . 881

26 Federation. . . . 883
26.1 Federation. . . . 883
26.2 Federation terms. . . . 884
26.3 Managing security rights. . . . 885
Rights required on the origin site. . . . 886
Rights required on the destination site. . . . 886
Federation-specific rights. . . . 887
Replicating security on an object. . . . 888
Replicating security using access levels. . . . 889
26.4 Replication types and mode options. . . . 889
One-way replication 889
Two-way replication 890
Refresh from origin or refresh from destination. . . . 890
26.5 Replicating third-party users and groups. . . . 892
26.6 Replicating universes and universe connections. . . . 893
26.7 Managing replication lists. . . . 894
Creating replication lists. . . . 895
Modifying Replication Lists. . . . 897
26.8 Managing remote connections. . . . 898
Creating remote connections. . . . 898
Modifying remote connections. . . . 900
26.9 Managing replication jobs. . . . 901
Creating replication jobs. . . . 901
Scheduling replication jobs. . . . 903
Modifying replication jobs. . . . 904
Viewing a log after a replication job. . . . 904
26.10 Managing object cleanup. . . . 905
How to use object cleanup. . . . 905

Object cleanup limits. . . . 906
Object cleanup frequency. . . . 906
26.11 Managing conflict detection and resolution. . . . 907
One-way replication conflict resolution. . . . 908
Two-way replication conflict resolution. . . . 909
26.12 Using Web Services in Federation. . . . 912
Session variables 913
File caching 913
Custom deployment 914
26.13 Remote scheduling and locally run instances. . . . 915
Remote scheduling. . . . 915
Locally run instances. . . . 916
Instance share. . . . 917
26.14 Importing and promoting replicated content. . . . 917
Importing replicated content. . . . 918
Importing replicated content and continuing replication 918
Promoting content from a test environment. . . . 919
Re-pointing a destination site. . . . 919
26.15 Best practices. . . . 920
Current release limitations. . . . 923
Troubleshooting error messages. . . . 924

27 Supplementary Configurations for ERP Environments. . . . 929
27.1 Configurations for SAP NetWeaver integration. . . . 929
Integrating with SAP Business Warehouse (BW). . . . 929
27.2 Configuring for PeopleSoft Enterprise integration. . . . 973
Configuring Single Sign-on (SSO) for SAP Crystal Reports and PeopleSoft Enterprise. . . . 973
Configuring Secure Sockets Layer communication. . . . 974
Performance Tuning for PeopleSoft systems. . . . 977

28 Managing and Configuring Logs. . . . 979
28.1 Logging traces for components. . . . 979
28.2 Trace log levels. . . . 979
28.3 Configuring tracing for servers. . . . 980
To set the log level in the CMC. . . . 980
To set the log level for multiple servers in the CMC. . . . 981
To configure server tracing using the BO_trace.ini file. . . . 982
28.4 Configuring tracing for web applications. . . . 985
To set the web application trace log level in the CMC. . . . 986
To configure tracing settings using the `BO_trace.ini` file. . . . 986
28.5 Configuring tracing for BI platform client applications. . . . 991
28.6 Configuring extended error message tracing. . . . 991

28.7 To enable error message extensive information log files. . . . 992

29 Integration to SAP Solution Manager. . . . 994
29.1 Integration overview. . . . 994
29.2 SAP Solution Manager integration checklist. . . . 994
29.3 Managing system landscape directory registration. . . . 995
Registration of the BI platform in the System Landscape. . . . 995
When is SLD registration triggered?. . . . 997
SLD Cleanup Before Patch Installations. . . . 997
Logging SLD connectivity 998
Virtual Hostname. . . . 998
29.4 Managing Solution Management Diagnostics agents. . . . 999
Solution Manager Diagnostics (SMD) overview. . . . 999
Working with SMD agents. . . . 999
SMAdmin user account. . . . 1000
29.5 Managing performance instrumentation. . . . 1000
Performance instrumentation for the BI platform. . . . 1000
Setting up performance instrumentation for the BI platform. . . . 1001
Performance instrumentation for the web tier. . . . 1002
Instrumentation log files 1002
29.6 Tracing with SAP Passport. . . . 1003

30 Command Line Administration. . . . 1004
30.1 Unix Scripts. . . . 1004
Script utilities. . . . 1004
Script templates. . . . 1009
Scripts used by the BI platform. . . . 1010
30.2 Windows scripts. . . . 1011
ccm.exe. . . . 1011
30.3 Server Command Lines. . . . 1014
Command lines overview. . . . 1014
Standard options for all servers. . . . 1015
Central Management Server. . . . 1016
Crystal Reports Processing Server and Crystal Reports Cache Server. . . . 1017
Job Servers. . . . 1018
Adaptive Processing Server. . . . 1019
Report Application Server. . . . 1019
Web Intelligence Processing Server. . . . 1020
Input and Output File Repository Servers. . . . 1022
Event Server. . . . 1023

31 Repository Diagnostic Tool. . . . 1025

31.1 Overview of the Repository Diagnostic Tool. . . . 1025
31.2 Using the Repository Diagnostic Tool. . . . 1025
To use the Repository Diagnostic Tool. . . . 1026
Repository Diagnostic Tool Parameters. . . . 1027
31.3 Inconsistencies between the CMS and the FRS. . . . 1035
31.4 Inconsistencies in the CMS metadata. . . . 1036
31.5 Managing Restful SDK inside BOE WebApp. . . . 1039

32 HTTP Strict Transport Security (HSTS). . . . 1041
32.1 Configuring HTTP Strict Transport Security (HSTS). . . . 1041

33 Rights Appendix. . . . 1042
33.1 About the rights appendix. . . . 1042
33.2 General rights. . . . 1042
Destination Rights. . . . 1045
33.3 Rights for specific object types. . . . 1046
Folder rights. . . . 1046
Categories. . . . 1046
Crystal reports. . . . 1047
Web Intelligence documents. . . . 1048
Users and groups. . . . 1048
Access levels. . . . 1050
Universe (.unx) rights. . . . 1050
Universe object-access levels. . . . 1051
Connection rights. . . . 1053
Applications. . . . 1054

34 Server Properties Appendix. . . . 1059
34.1 About the server properties appendix. . . . 1059
Common Server Properties. . . . 1059
Core Services properties. . . . 1061
Connectivity Services Properties. . . . 1066
Crystal Reports Services Properties. . . . 1070
Data Federation Services Properties. . . . 1077
Web Intelligence Services properties. . . . 1078

35 Server Metrics Appendix. . . . 1085
35.1 About the Server Metrics Appendix. . . . 1085
Common Server Metrics 1085
Central Management Server Metrics. . . . 1087
Connection Server Metrics. . . . 1090
Event Server Metrics. . . . 1091
File Repository Server Metrics. . . . 1091

Adaptive Processing Server Metrics. 1092
Adaptive Job Server Metrics. 1096
Crystal Reports Server Metrics. 1097
Web Intelligence Server Metrics. 1100

36 Server and Node Placeholder Appendix. 1102
36.1 Server and node placeholders. 1102

37 Auditing Data Store Schema Appendix. 1111
37.1 Overview. 1111
37.2 Schema diagram. 1111
37.3 Auditing Data Store Tables. 1111

38 Monitoring Database Schema Appendix. 1119
38.1 Trending database schema. 1119

39 System Copy Worksheet Appendix. 1122
39.1 System copy worksheet. 1122

1 Document History

The following table provides an overview of the most important document changes.

Version	Date	Description
SAP BusinessObjects Business Intelligence platform 2025	March 2025	For detailed information, see .
SAP BusinessObjects Business Intelligence platform 4.3 SP3	December 2022	Updated the following topics with the new maximum password length field for enterprise authentication: • Enterprise authentication settings [page 231] • To create a user account [page 90] • To change general password settings [page 101] • To change general password settings [page 233] • Introduced enable Use Relative URL path option to use the relative url of the browser.
SAP BusinessObjects Business Intelligence platform 4.3 SP2	December 2021	Added Authorization Server Configuration [page 672]. Updated Customizing Web Intelligence interface elements by user groups and folders [page 695].

SAP BusinessObjects Business Intelligence platform 4.3 SP1	December 2020	• Added the following new topics:
		  • A topic about Web Intelligence UI customization. See Customizing Web Intelligence interface elements by user groups and folders [page 695].
		  • Script to clear Stale Sessions [page 150].
		  • Define the database credentials against a data source reference for a user in BI Launch Pad [page 392]
		  • JMX SSL Configuration [page 743]
		• Updated two topics:
		  • Upgrade Paths [page 27].
		  • Destination Rights [page 1045] for *Destination Options* and *Email destination properties* with the newly introduced *Reply To* field for all publication scenarios.

SAP BusinessObjects Business Intelligence platform 4.3	June 2020	• SAP BusinessObjects Explorer, SAP BusinessObjects Dashboards, Report Conversion Tool, Upgrade Management Tool and BI Widgets have been deprecated in the 4.3 release. • Added a new topic Workflow Assistant [page 768].

2 Getting Started

2.1 About this guide

This guide provides you with information and procedures for deploying and configuring SAP BusinessObjects Business Intelligence platform (the "BI platform"). Procedures are provided for common tasks. Conceptual information and technical details are provided for all advanced topics.

For information about installing this product, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*.

2.1.1 Who should use this guide?

This guide covers deployment and configuration of the BI platform. We recommend consulting this guide if you are performing any of the following tasks:

- Planning your first deployment
- Configuring your first deployment
- Making significant changes to the architecture of an existing deployment
- Improving your system's performance

This guide is intended for system administrators who are responsible for configuring, managing, and maintaining a BI platform installation. Familiarity with your operating system and your network environment is beneficial, as is a general understanding of web application server management and scripting technologies. However, to assist all levels of administrative experience, this guide aims to provide sufficient background and conceptual information to clarify all administrative tasks and features.

2.1.2 About the Business Intelligence platform

The Business Intelligence (BI) platform is a flexible and scalable solution for delivering information to end users, in multiple forms including dashboards and interactive reports, via any web application—intranet, extranet, Internet, or corporate portal.

The platform delivers tangible benefits extending across and beyond the organization, as an integrated suite for reporting, analysis, and information delivery.

It also provides a solution for increasing end-user productivity and reducing administrative efforts.

For example, it is used to distribute weekly sales reports, to provide customers with personalized service offerings, or to integrate critical information in corporate portals.

2.1.3 Variables

The following variables are used throughout this guide.

Variable	Description
`<INSTALLDIR>`	The directory where the BI platform is installed. On Windows, the default directory is `C:\Program Files (x86)\SAP BusinessObjects\`.
`<PLATFORM64DIR>`	The name of your Unix operating system. Acceptable value is linux_x64.
`<SCRIPTDIR>`	The directory where scripts for administering the BI platform are located. On Windows, the directory is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`. On Unix, the directory is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64DIR>/scripts`.

2.1.4 Terminology

The following terms are used throughout the BI platform documentation:

Term	Definition
Add-on products	Products that work with the BI platform but have their own installation program.
Auditing Data Store (ADS)	The database used to store auditing data
BI platform	An abbreviation for the SAP BusinessObjects Business Intelligence platform
Bundled database; bundled web application server	The database or web application server shipped with the BI platform
Cluster (noun)	Two or more Central Management Servers (CMSs) working together and using a single CMS database
Cluster (verb)	To create a cluster: 1. Install a CMS and CMS database on machine A. 2. Install a CMS on machine B. 3. Point the CMS on machine B to the CMS database on machine A.

Term	Definition
Cluster key	Used to decrypt the keys in the CMS database. You can change the cluster key in the CCM, but you cannot reset the key like a password. It contains encrypted content and is important not to lose.
CMS	An abbreviation for the Central Management Server
CMS database	The database used by the CMS to store information about the BI platform
Deployment	The BI platform software installed, configured, and running on one or more machines
Installation	An instance of BI platform files created by the installation program on a machine
Machine	The computer on which the BI platform software is installed
New BI release	A full release or release of some components of software
Node	A group of BI platform servers that run on the same machine and are managed by the same Server Intelligence Agent (SIA)
Patch	A small update for a specific BI release version
Promotion	The process of transferring BI content between deployments with the same BI release, using the promotion management application
Server	A BI platform process. A server hosts one or more services
Server Intelligence Agent (SIA)	A process that manages a group of servers, including stopping, starting, and restarting servers
Web application server	A server that processes dynamic content
Upgrade	The planning, preparation, migration, and post-processes required to complete a migration process
ONE Installer	ONE Installer is a single installation package that supports multiple BI installation scenarios such as, fresh installation of a New BI release or Patch, any Patch to Patch update, or any BI release to Patch update.

2.2 Before you start

2.2.1 Key concepts

2.2.1.1 Server Intelligence

Server Intelligence is a core component of the BI platform. Changes to server processes applied in the Central Management Console (CMC) are propagated to corresponding server objects by the Central Management Server (CMS). The Server Intelligence Agent (SIA) is used to automatically restart or shut down a server if it encounters an unexpected condition, and is accessed by an administrator when managing the node.

The CMS stores information about servers in the CMS system database so you can easily restore default server settings. Because the SIA periodically queries the CMS to request information about servers it manages, the SIA knows which state servers should be in and when to take action.

> ⓘ Note
>
> A BI platform installation is a unique instance of the BI platform files created by the installer on a machine. An instance of a BI platform installation can be used only within a single cluster. Nodes belonging to different clusters sharing the same BI platform installation are not supported because this type of deployment cannot be patched or updated. Only Unix platforms support multiple installations of the software on the same machine. If each installation is performed under a unique user account, and is installed to a separate folder, the installations do not share any files. Remember that all machines in the cluster must have the same version and patch level.

Related Information

Servers, hosts, and clusters [page 35]

2.2.1.2 Servers, services, nodes, and hosts

The BI platform uses the terms server and service to refer to the two types of software running on a BI platform computer.

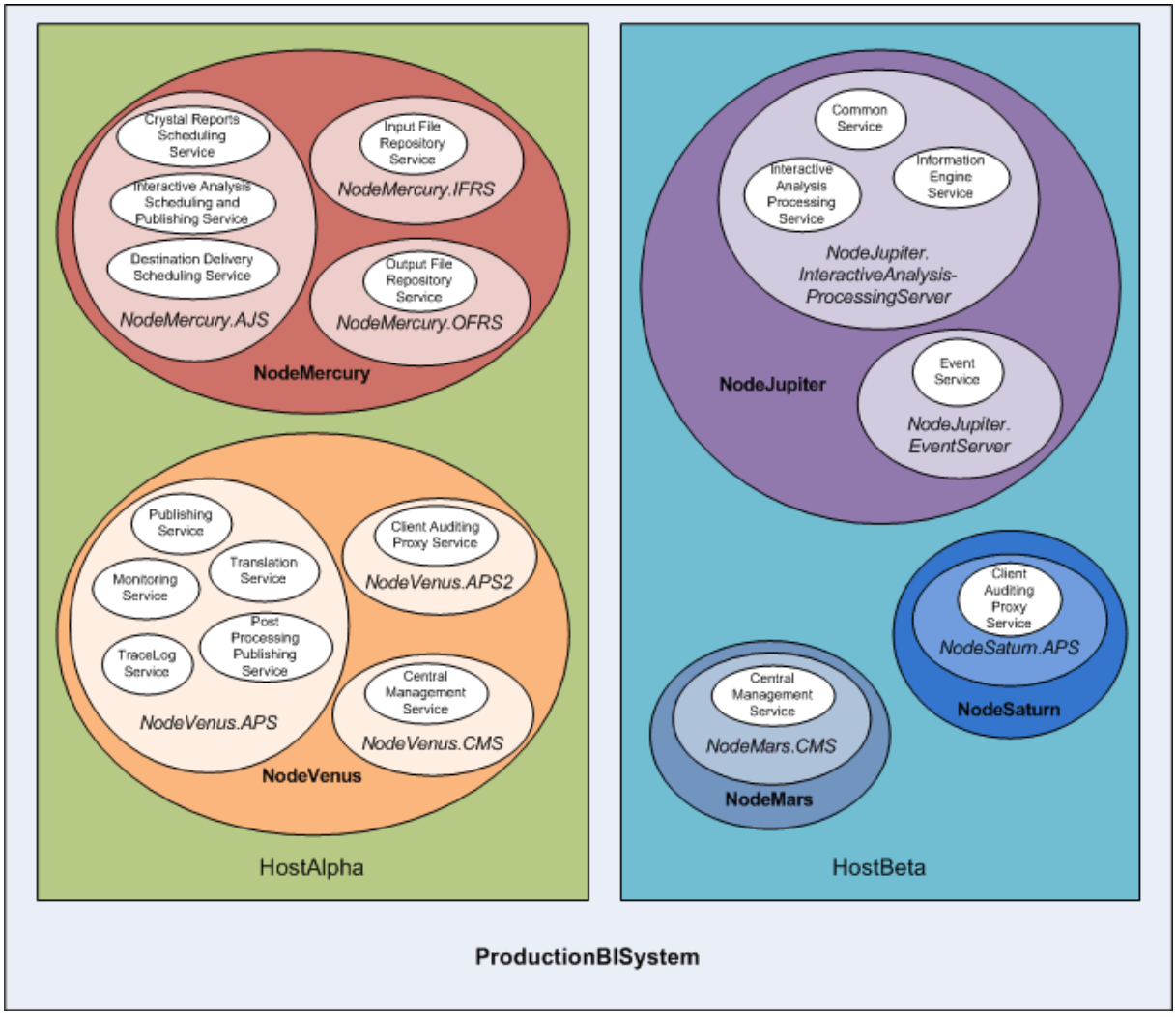
The term “server” is used to describe an operating-system-level process (on some systems, this is referred to as a daemon) that hosts one or more services. For example, the Central Management Server (CMS) and Adaptive Processing Server are servers. A server runs under a specific operating system account and has its own process ID (PID).

A service is a server subsystem that performs a specific function. The service runs within the memory space of its server under the process ID of the parent container (server). For example, the Web Intelligence Scheduling Service is a subsystem that runs within the Adaptive Job Server.

A node is a collection of BI platform servers running on the same host and managed by the same Server Intelligence Agent (SIA). One or more nodes can be on a single host.

The BI platform can be installed on a single computer, spread across different computers on an intranet, or separated over a wide area network (WAN).

The following diagram shows a hypothetical installation of the BI platform. The number of hosts, nodes, servers, and services—as well as the type of servers, and services—varies in actual installations.



Two hosts form the cluster named ProductionBISystem:

- The host named HostAlpha has the BI platform installed and is configured to have two nodes:
  - NodeMercury contains an Adaptive Job Server (`NodeMercury.AJS`) with services to schedule and publish reports, an Input File Repository Server (`NodeMercury.IFRS`) with a service to store input reports, and an Output File Repository Server (`NodeMercury.OFRS`) with a service to store report output.

- NodeVenus contains an Adaptive Processing Server (`NodeVenus.APS`) with services to provide publishing, monitoring, and translation features, an Adaptive Processing Server (`NodeVenus.APS2`) with a service to provide client auditing, and a Central Management Server (`NodeVenus.CMS`) with a service to provide the CMS services.

- The host named HostBeta has the BI platform installed and is configured to have three nodes:
  - NodeMars contains a Central Management Server (`NodeMars.CMS`) with a service to provide the CMS services. Having the CMS on two computers enables load balancing and mitigation and failover capabilities.
  - NodeJupiter contains a Web Intelligence Processing Server (`NodeJupiter.Web Intelligence`) with a service to provide Web Intelligence reporting, and an Event Server (`NodeJupiter.EventServer`) to provide report monitoring of files.
  - NodeSaturn contains an Adaptive Processing Server (`NodeSaturn.APS`) with a service to provide client auditing.

2.2.2 Key administrative tools

2.2.2.1 System Configuration Wizard

The System Configuration Wizard is a tool that you can use to configure your BI platform deployment simply and quickly. The wizard guides you through the basic configuration options, resulting in a working deployment using common settings such as these:

- Which products' servers you want to start automatically with the BI platform
- Whether you want to optimize your deployment for maximum performance, or for limited hardware resources
- The locations of system folders

By default, the wizard is set to run automatically when you log in to the Central Management Console (CMC), but you can change this setting in the wizard. You can also start the wizard at any time from the *Manage* area in the CMC.

> **Note**
>
> In production systems, it is a good practice to set the wizard not to run automatically, to prevent accidental reconfiguration.

> **Note**
>
> It is recommended that you perform a full backup before using the wizard to make changes to an existing system.

2.2.2.2 Central Management Console (CMC)

The Central Management Console (CMC) is a web-based tool that you use to perform administrative tasks (including user, content, and server management) and to configure security settings. Because the CMC is a

web-based application, you can perform all of the administrative tasks in a web browser on any computer that can connect to the web application server.

Only members of the Administrators group can change management settings, unless a user is explicitly granted rights to do so. Roles can be assigned in the CMC to grant user privileges to perform minor administrative tasks, such as managing users in your group and managing reports in folders that belong to your team.

2.2.2.3 Central Configuration Manager (CCM)

The Central Configuration Manager (CCM) is a server troubleshooting and node management tool provided in two forms. In a Microsoft Windows environment, the CCM allows you to manage local and remote servers through its graphical user interface (GUI) or from a command line. In a Unix environment, the CCM shell script (`ccm.sh`) allows you to manage servers from the command line.

You use the CCM to create and configure nodes and to start or stop your web application server, if it is the default bundled Tomcat web application server. On Windows, it also allows you to configure network parameters, such as Secure Sockets Layer (SSL) encryption. These parameters apply to all servers within a node.

> **Note**
>
> Most server management tasks are now handled through the CMC, not through the CCM. The CCM is now used for troubleshooting and node configuration.

2.2.2.4 Repository Diagnostic Tool

The Repository Diagnostic Tool (RDT) can scan, diagnose, and repair inconsistencies that may occur between the Central Management Server (CMS) system database and the File Repository Servers (FRS) filestore. You can set a limit for the number of errors the RDT will find and repair before stopping.

The RDT should be used after you restore your BI platform system.

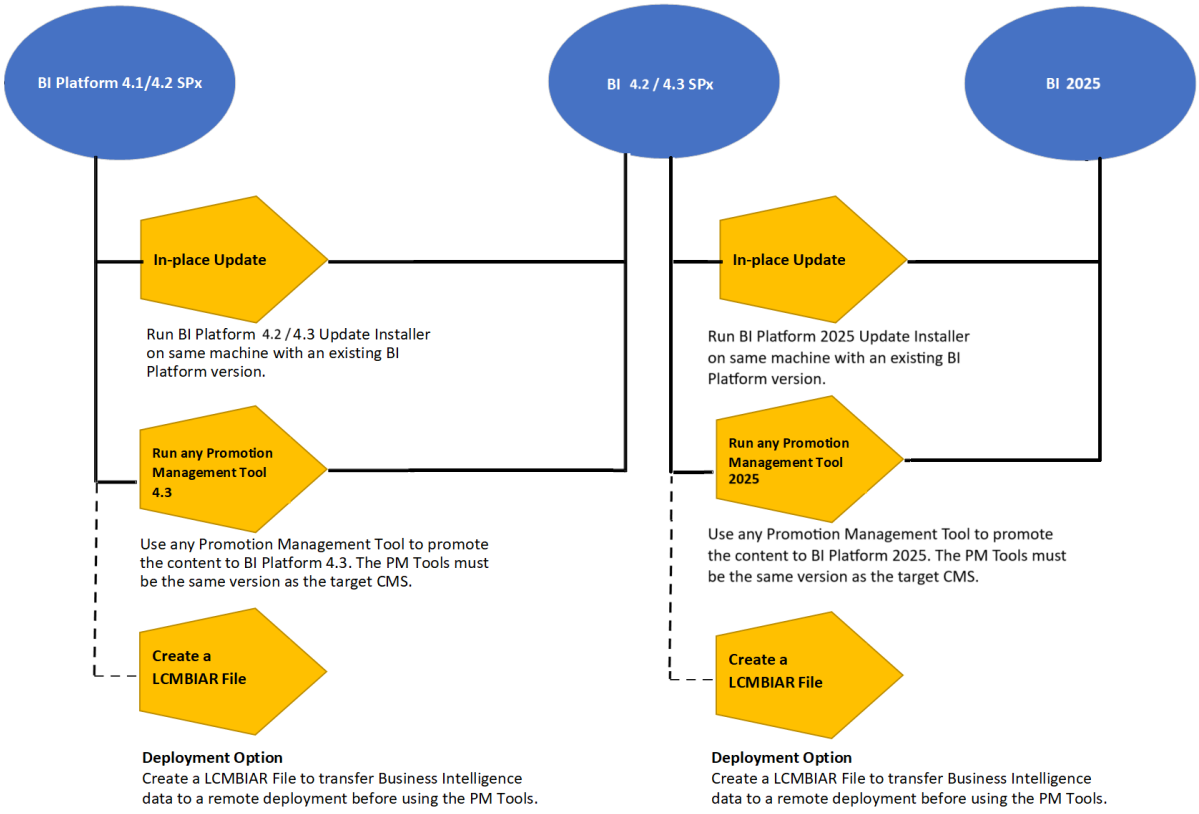
> **Note**
>
> On production systems, it is a good practice to regularly run the RDT but with the “repair” option disabled, to watch for any underlying system health issues. Run the RDT with the repair option enabled only if you are sure you want the RDT to execute repairs to your system.

2.2.2.5 Upgrade Management Tool

UMT is being deprecated in BI 4.3 release. For more details, please refer to 2801797

2.2.2.6 Upgrade Paths

You can migrate your system data and business intelligence content from the previous BI 4.x versions to SAP BusinessObjects Business Intelligence platform 4.3.



The Upgrade Management Tool is deprecated in SAP BusinessObjects Business Intelligence platform 4.3, however, you can follow the below mentioned upgrade paths to move to 4.3.

If you have an older deployment, follow these guidelines to upgrade your existing deployment to BI platform 4.3:

1. If your existing deployment is of XI R2, XI MHF1, XI R2 SP1, BusinessObjects 5/6, or Crystal Enterprise 9/10, you must first upgrade to XI R2 SP2 (or higher) and proceed from step 3
2. If your existing deployment is of XI 3.x, you can directly proceed with the upgrade from step 3
3. Install BI 4.1/4.2 SPx on a separate machine, and run Upgrade Management Tool from the 4.1/4.2 SPx to migrate the content from the above-mentioned versions to BI 4.1/4.2 SPx level
4. Once you have your content in BI 4.1/4.2 SPx level, you can choose either of the following methods to move to 4.3
    1. Run the update installation software of BI 4.3.x on the machine at 4.1/4.2 SPx level, or

2. Install BI 4.3 on a separate machine and use the Promotion Management Tool from BI 4.3.x to promote the content from the BI 4.1/4.2 SPx level to BI 4.3.x level

> **Note**
>
> 1. To promote the content from the BI 4.1/4.2 SPx level to BI 4.3.x level, the Promotion Management tool must be of the same version as the target CMS.
> 2. For more information on the BusinessObjects 5/6 to XI 3.1, refer the Migration Guide and the BI platform Installation Guide for your version available at https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_ENTERPRISE_BUSINESS_INTELLIGENCE_PLATFORM/XI.3.1/en-US.
> 3. The Upgrade Management Tool (UMT) upgrades only the Server and Web Tier features in your deployment. For more information on UMT, see the Business Intelligence Platform Upgrade Guide for your version, available at https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_BUSINESS_INTELLIGENCE_PLATFORM/4.2/en-US.

2.2.3 Key tasks

Depending on your situation, you may want to focus on specific sections of this guide, and there may be other resources available for you. For each of the following situations, there is a list of suggested tasks and reading topics.

Related Information

Planning or performing your first deployment [page 28]
Configuring your deployment [page 29]
Improving your system's performance [page 29]
Central Management Console (CMC) [page 25]

2.2.3.1 Planning or performing your first deployment

If you are planning or performing your first deployment of the BI platform, it is recommended that you read these sections in this guide:

- To get familiar with the BI platform components, read “Architecture overview”
- “Understanding communication between BI platform components”
- “Security overview”
- If you will use third-party authentication, read “Authentication options in the BI platform”
- After you install, read “Working with the Servers management area in the CMC”

For more information about installing the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. To assess your needs and design a deployment architecture that works best for you, read the *SAP BusinessObjects Business Intelligence Platform Planning Guide*.

Related Information

Architecture overview [page 31]
Communication between BI platform components [page 188]
Security overview [page 142]
Authentication options in the BI platform [page 226]
Working with the Servers management area in the CMC [page 402]

2.2.3.2 Configuring your deployment

If you have just completed your installation of the BI platform and need to perform initial configuration tasks, such as firewall configuration and user management, it is recommended that you read the following sections.

Related Information

Introduction to the System Configuration Wizard [page 76]
Communication between BI platform components [page 188]
Security overview [page 142]
Monitoring [page 727]

2.2.3.3 Improving your system's performance

If you want to assess your deployment's efficiency and to fine-tune it to maximize resources, read the following sections:

- If you want to use a deployment template to configure your system, read “Introduction to the System Configuration Wizard”.
- If you want to monitor your existing system, read “About monitoring”.
- For daily maintenance tasks and procedures for working with servers in the CMC, read “Working with the Servers management area in the CMC”.

Related Information

Introduction to the System Configuration Wizard [page 76]
Monitoring [page 727]
Working with the Servers management area in the CMC [page 402]

2.2.3.4 Working with objects in the CMC

An object is a document or file created in the BI platform or other software, that is stored and managed in the BI platform repository. If you are working with objects in the CMC, read the following sections:

- For information about setting up users and groups in the CMC, see “Account management overview”.
- To set security on objects, see “How rights work in the BI platform”.
- For general information about working with objects, see *SAP BusinessObjects Business Intelligence Platform User's Guide*.

Related Information

Account management overview [page 88]
How rights work in BI platform [page 115]

3 Architecture

3.1 Architecture overview

This section outlines the overall platform architecture, system, and service components that make up the SAP BusinessObjects Business Intelligence platform. The information helps administrators understand the system essentials and helps to form a plan for the system deployment, management, and maintenance.

> **Note**
>
> For a list of supported platforms, languages, databases, web application servers, web servers, and other systems supported by this release, see the *Product Availability Matrix* (PAM), available at http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540.

> **Note**
>
> Because the PAM is continually updated, always refer to the online version of the PAM instead of a downloaded copy.

The Business Intelligence (BI) platform is designed for high performance across a broad spectrum of user and deployment scenarios. You can offload processor intensive scheduling and processing by creating dedicated servers to host specific services. The architecture is designed to meet the needs of virtually any BI deployment, and is flexible enough to grow from several users with a single tool, to tens of thousands of users with multiple tools and interfaces.

Developers can integrate the BI platform into their organization's other technology systems by using web services, Java, or .NET application programming interfaces (APIs).

End users can access, create, edit, and interact with reports using specialized tools and applications that include:

- Clients installed by the BI platform Client Tools installation program:
  - Web Intelligence Rich Client
  - Business View Manager
  - Information Design Tool (formerly Information Designer)
  - Translation Management Tool (formerly Translation Manager)
- Clients available separately:
  - SAP Crystal Reports
  - SAP BusinessObjects Analysis (formerly Voyager)
  - BI Workspaces (formerly Dashboard Builder)

IT departments can use data and system management tools that include:

- Report viewers
- Central Management Console (CMC)
- Central Configuration Manager (CCM)

- Repository Diagnostic Tool (RDT)
- Data Federation Administration Tool

To provide flexibility, reliability, and scalability, BI platform components can be installed on one or across many machines. In some cases, you can even install two different versions of the BI platform simultaneously on the same computer, although this configuration is only recommended as part of the upgrade process or for testing purposes.

Server processes can be vertically scaled (where one computer runs several, or all, server-side processes) to reduce cost, or horizontally scaled (where server processes are distributed between two or more networked machines) to improve performance. It is also possible to run multiple, redundant, versions of the same server process on more than one machine, so that processing can continue if the primary process encounters a problem.

> **Note**
>
> While it is possible to use a mixture of Windows and Unix or Linux platforms, it is recommended that you do not mix operating systems for Central Management Server (CMS) processes.

3.1.1 Component diagram

SAP BusinessObjects Business Intelligence platform is a Business Intelligence (BI) platform that provides enterprise-level analysis and reporting tools to facilitate information delivery. Data can be analyzed from any of a large number of supported database systems (including text or multi-dimensional OLAP systems) and BI reports can be published in many different formats to many different publishing systems.

This architecture diagram illustrates the BI platform components, including servers and client tools, and additional analytic products, web application components, and databases that can be part of a BI platform landscape: BI 2025 Architecture Diagram.

The BI platform reports from a read-only connection to your organization's databases, and uses its own databases for storing its configuration, auditing, and other operational information. The BI reports created by the system can be sent to a variety of destinations, including file systems, and email, or accessed through web sites or portals.

The BI platform is a self-contained system that can exist on a single machine (for example, as a small development or pre-production test environment) or can be scaled up into a cluster of many machines that run different components (for example, as a large-scale production environment).

3.1.2 Architecture tiers

SAP BusinessObjects Business Intelligence platform can be thought of as a series of conceptual tiers:

Client tier

The client tier contains all desktop client applications that interact with the BI platform to provide a variety of reporting, analytic, and administrative capabilities. Examples include the Central Configuration Manager (BI

platform installation program), Information design tool (BI platform Client Tools installation program), and SAP Crystal Reports (available and installed separately).

As of SAP BI 4.3, desktop client applications (Web Intelligence Rich Client, Information Design Tool, Universe Design Tool,...) are 64-bit applications. They are and no longer 32-bit.

Web tier

The web tier contains web applications deployed to a Java web application server. Web applications provide BI platform functionality to end users through a web browser. Examples of web applications include the Central Management Console (CMC) administrative web interface and BI launch pad.

The web tier also contains Web Services. Web Services provides BI platform functionality to software tools via the web application server, such as session authentication, user privilege management, scheduling, search, administration, reporting, and query management. For example, Live Office is a product that uses Web Services to integrate BI platform reporting into some Microsoft Office products.

Management tier

The management tier (also known as intelligence tier) coordinates and controls all of the components that make up the BI platform. It comprises the Central Management Server (CMS) and the Event Server and associated services. The CMS maintains security and configuration information, directs service requests to servers, manages auditing, and maintains the CMS system database. The Event Server manages file-based events, which occur in a defined storage tier.

Storage tier

The storage tier is responsible for handling files, such as documents and reports.

The Input File Repository Server manages files that contain information to be used in reports, such as the following file types: `.rpt`, `.car`, `.exe`, `.bat`, `.js`, `.xls`, `.doc`, `.ppt`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`, `.unv`, `.unx`.

> **Note**
>
> The size of the Input File Repository Server file store is not managed by the system; therefore, an administrator should manage a monitoring and maintenance plan.

The Output File Repository Server manages reports created by the system, such as the following file types: `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`.

The storage tier also handles report caching to save system resources when users access reports.

Processing tier

The processing tier analyzes data, and produces reports and other output types. This is the only tier that accesses the databases that contain report data. This tier comprises the Adaptive Job Server, Connection Server (64-bit), and processing servers such as the Adaptive Processing Server or Crystal Reports Processing Server.

Data tier

The data tier consists of the database servers hosting the CMS system database and Auditing Data Store. It also consists of any database servers containing relational, OLAP, or other data types for reporting and analytic applications.

3.1.3 Databases

The BI platform uses several different databases.

- Reporting database
  This refers to your organization's data. It is the source data analyzed and reported on by SAP BusinessObjects Business Intelligence Suite products. Most commonly, the data is stored within a relational database, but it can also be contained within text files, Microsoft Office documents, or OLAP systems.
- CMS system database
  The CMS system database is used to store BI platform information, such as user, server, folder, document, configuration, and authentication details. It is maintained by the Central Management Server (CMS), and is sometimes referred to as the *system repository*.
- Auditing Data Store
  The Auditing Data Store (ADS) is used to store information on trackable events that occur in the BI platform. This information can be used to monitor the usage of system components, user activity, or other aspects of day-to-day operation.
- Monitoring database
  Monitoring uses the Auditing Data Store (ADS) database to store system configuration and component information for SAP supportability.
- Commentary Database
  The BI Commentary is an application that is introduced in the CMC. It allows users to collaborate by commenting on any of the data/statistics available in a given document.
  Commentary database is configured in the same database as Auditing database. It gets created by default in the Auditing database.

If you do not have a database server in place for use with the CMS system and Auditing Data Store databases, the BI platform installation program can install and configure one for you. It is recommended that you evaluate your requirements against information from your database server vendor to determine which supported database would best suit your organization's requirements.

> **Note**
>
> The default SQL Anywhere database is not recommended for production systems. It is bundled with the BI platform server packages that enables you to deploy and test the BI platform instantly, but has limited capabilities required to manage a database. It is recommended to use SQL Anywhere in its complete form, or an existing supported database instance for production system as this is critical for your CMS database to reside in your data center. It is managed by database administrators with appropriate processes established for data security and availability of servers.

3.1.4 Servers, hosts, and clusters

The BI platform consists of collections of servers running on one or more hosts. Small installations (such as test or development systems) can use a single host for a web application server, database server, and all BI platform servers.

Medium and large installations can have servers running on multiple hosts. For example, a web application server host can be used in combination with a BI platform server host. This frees up resources on the BI platform server host, allowing it to process more information than if it also hosted the web application server.

Large installations can have several BI platform servers hosts working together in a cluster. For example, if an organization has a large number of SAP Crystal Reports users, Crystal Reports processing servers can be created on multiple BI platform servers hosts to ensure that there are plenty of resources available to process requests from clients.

The advantages of having multiple servers include:

- Improved performance
  Multiple BI platform server hosts can process a queue of reporting information faster than a single BI platform server host.
- Load balancing
  If a server is experiencing a heavy load, the CMS automatically sends new work to other servers in the cluster.
- Improved availability
  If a server encounters an unexpected condition, the CMS automatically re-routes work to different servers until the condition is corrected.

3.1.5 Web application servers

A web application server acts as the translation layer between a web browser or rich application, and the BI platform. Web application servers running on Windows, Unix, and Linux are supported.

For a detailed list of supported web application servers, consult the *Supported Platforms/PARs*, available at: https://support.sap.com/home.html.

If you do not have a web application server in place for use with the BI platform, the installation program can install and configure a Tomcat web application server for you. It is recommended that you evaluate your requirements against information from your web application server vendor to determine which supported web application server would best suit your organization's requirements.

> **Note**
>
> When configuring a production environment, it is recommended that the web application server is hosted on a separate system. Running the BI platform and a web application server on the same host in a production environment may decrease performance.

3.1.5.1 Enabling Clustering in BI Launchpad Web Application to Support Session Failover and Scalability

This section describes how to enable clustering in the BI Launchpad web application to support session failover and scalability. This section also explains the steps for configuring Apache Tomcat application servers for the same purpose.

Prerequisites

To enable clustering for any application server such as Tomcat, you need the following components:

- A HTTP server
- A compatible load balancer
- Two or more instances of the application server with the required Web application already installed
- A complete BOE installation (repository)

Context

> **Note**
>
> The steps described in this section are generic and can be used to enable clustering for any other application. The only differences are the changes made in the deployment descriptor of the web-app (web.xml). We recommend consulting your web application sever vendor to know how to set up web tier load balancing.

3.1.5.1.1 Installing Apache Tomcat

Context

To install Apache Tomcat server, perform the following steps:

Procedure

1. Install Apache HTTP server.
2. Install Apache Tomcat Server in the instance machines.
3. Download mod_jk (loadbalancer) and save it in the "modules" directory on the Apache HTTPD server from http://tomcat.apache.org/download-connectors.cgi .
4. Run SI agent on a machine, which has a full installation of BOE already installed.

> **Note**
>
> To check the compatibility for mod_jk, start your HTTP server. An error message appears on the console if the downloaded version of mod_jk is not compatible with your version of HTTP server.

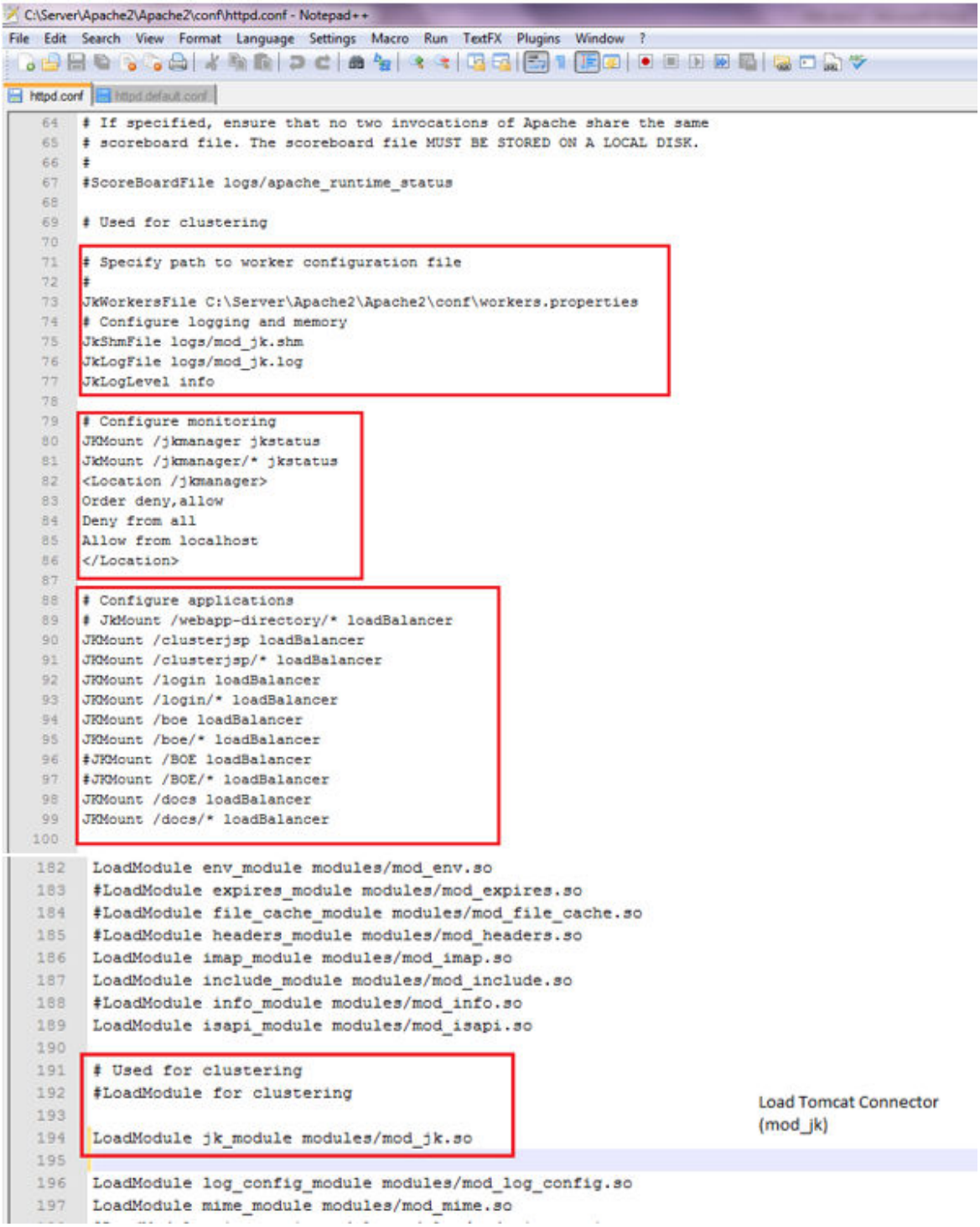
Configuring Apache Tomcat

Context

To configure Apache Tomcat, perform the following steps:

Procedure

1. Configure Apache HTTP server.
   a. Configure httpd.conf (load balancer, load web app, monitoring, path to worker.properties file).
   b. Configure the workers.properties file and save it in the Apache\Conf library.



2. Configure server.xml in Tomcat (add clustering tags).
   a. In server.xml, the jvmRoute attribute should correspond to the name you have used in the workers.properties file.
   b. If you are using Tomcat 8 or above, remove JvmRouteSessionIDBinderListener (deprecated).
3. Add a distributable tag to the web.xml file (deployment descriptor) of the web app, in which you want clustering to be supported.

The custom valve, which invokes the default valve for every request, is specified below. If you're using Tomcat 8, in all the Tomcats server.xml, replace:

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Inte
rceptor"/>
```

with

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatchInterc
eptor"/>
```

```
    <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
  </Channel>

  <Valve className="com.sap.customvalve.ForceReplicationValve"/>
   <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=".*\.gif;.*\.jpg;.*\.png;.*\.js;.*\.htm
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer" deployDir="/tmp/war-deploy/" tempDir="/tmp
```

4. Export the jar for the custom valve (if modifications are needed) from the code. Copy the `forcereplicationvalve.jar` file in `<BOEInstallDir>/SAP BusinessObjects XI 4.0/java/lib` and paste it in `<TomcatInstallDir>/tomcat/lib` (in all Tomcat nodes).
5. Store this jar in the `tomcat/lib` folder of each instance.
6. Restart all the servers.

> **Note**
>
> - As a best practice, we recommend that you start servers one at a time; wait until one server has been completely started before starting another.
> - Do not use localhost:6400 as the system name in the login screen for Launchpad. Provide the name (or IP) of the specific BOE installation machine. Make sure that SI agent is running on this installation.
> - Explore channelSendOptions attribute for the most suitable option. It is used to set options for synchronous response, asynchronous response and so on.
> - When exporting the jar for custom valve from the code, remember to create a proper package hierarchy for the jar and include this hierarchy in server.xml.

3.1.6 Software Development Kits

A Software Development Kit (SDK) allows a developer to incorporate aspects of SAP BusinessObjects Business Intelligence platform into an organization's own applications and systems.

The BI platform has SDKs for software development on Java and .NET platforms.

> **Note**
>
> The BI platform .NET SDKs are not installed by default, and must be downloaded from the SAP Service Marketplace.

The following SDKs are supported by the BI platform:

- Business Intelligence platform Java SDK and .NET SDK
  The BI platform SDKs allow applications to perform tasks such as authentication, session management, working with repository objects, report scheduling and publication, and server management.

  > **Note**
  >
  > For full access to security, server management, and auditing functions, use the Java SDK.

- Business Intelligence platform RESTful web service SDK
  The BI platform RESTful web service SDK lets you access the BI platform using the HTTP protocol. You can use this SDK to log on to the BI platform, navigate the BI platform repository, access resources, and perform basic resource scheduling. You can access this SDK by writing applications that use any programming language that supports the HTTP protocol, or by using any tool that supports making HTTP requests.
- Business Intelligence platform Java Consumer SDK and .NET Consumer SDK
  An implementation of SOAP-based Web Services that allows you to handle user authentication and security, document and report access, scheduling, publications, and server management.
  BI platform Web Services uses standards such as XML, SOAP, AXIS 2.0 and WSDL. The platform follows WS-Interoperability Basic Profile 1.0 web services specification.

  > **Note**
  >
  > Web Services applications are currently only supported with the following load balancer configurations:
  > 1. Source IP address persistence.
  > 2. Source IP and destination port persistence (available only on a Cisco Content Services Switch).
  > 3. SSL persistence.
  > 4. Cookie based session persistence.

  > **Note**
  >
  > SSL persistence may cause security and reliability issues on some web browsers. Check with your network administrator to determine if SSL persistence is appropriate for your organization.

- Data Access Driver and Connection Java SDKs
  These SDKs allow you to create database drivers for the Connection Server and manage database connections.
- Semantic Layer Java SDK
  The Semantic Layer Java SDK allows you to develop a Java application that performs administration and security tasks on universes and connections. For example, you can implement services for publishing a universe to a repository or retrieving a secured connection from the repository to your workspace. This application can be embedded within BI platform solutions that integrate the BI platform as OEM.
- Report Application Server Java SDK and .NET SDK
  The Report Application Server SDKs allow applications to open, create, and modify existing Crystal reports, including setting parameter values, changing data sources, and exporting to other formats, including XML, PDF, Microsoft Word, and Microsoft Excel.

- Java and .NET Crystal Reports Viewers
  The viewers allow applications to display and export Crystal reports. The following viewers are available:
  - DHTML Report Page Viewer: presents data and allows drill-down, page navigation, zooming, prompting, search, highlighting, exporting, and printing.
  - Report Parts Viewer: provides the ability to view individual parts of a report, including charts, text, and fields.
- Report Engine Java SDK and .NET SDK
  The Report Engine SDKs allow applications to interact with reports created with SAP BusinessObjects Web Intelligence.
  The Report Engine SDKs include libraries that you can use to build a web report design tool. Applications built with these SDKs can view, create, or modify, a variety of different Web Intelligence documents. Users can modify documents by adding, removing, and modifying objects such as tables, charts, conditions, and filters.
- Platform Search SDK: The Platform Search SDK is the interface between the client application and the Platform Search Service. Platform Search supports Public SDK that comes as a part of the Platform Search SDK.
  When a search request parameter is sent through the client application to the SDK layer, the SDK layer converts the request parameter into XML- encoded format and passes it to the Platform Search Service.

The SDKs can be used in combination to provide a wide range of BI functionality to your applications. For more information on these SDKs, including developer guides and API references, see the SAP BusinessObjects Business Intelligence Platform product page.

3.1.7 Data sources

3.1.7.1 Universes

The universe is a semantic layer that abstracts the data complexity by using business language rather than data language to access, manipulate, and organize data. This business language is stored as objects in a universe file. Web Intelligence, Crystal Reports, and other applications use universes to simplify the user creation process required for simple to complex end-user query and analysis.

Universes are a core component of the BI platform. All universe objects and connections are stored and secured in the central repository by the Connection Server. Client tools for designing universes need to log into the BI platform to access the system and create universes. Universe access and row/column-level security can also be managed at the group or individual user level from within the design environment.

The semantic layer allows Web Intelligence to deliver documents, by utilizing multiple synchronized data providers, including online analytical processing (OLAP) and common warehousing metamodel (CWM) data sources.

3.1.7.2 Business Views

Business Views simplify report creation and interaction by abstracting the complexity of data for report developers. Business Views help separate the data connections, data access, business elements, and access control.

Business Views can only be used by Crystal Reports and are designed to simplify the data access and view-time security required for Crystal report creation. Business Views support the combination of multiple data sources in a single view. Business Views are fully supported in the BI platform.

3.1.8 Authentication and single sign-on

System security is managed by the Central Management Server (CMS), security plug-ins, and third-party authentication tools, such as SiteMinder or Kerberos. These components authenticate users and authorize user access to the BI platform, its folders, and other objects.

The following user authentication single sign-on security plug-ins are available:

- Enterprise (default), including Trusted Authentication support for use with authentication methods like SAML, X.509, SAP NW SSO, and other methods supported by your application server.
- LDAP
- Windows Active Directory (AD)

When using an Enterprise Resource Planning (ERP) system, single sign-on is used to authenticate user access to the ERP system so that reports can source ERP data. The following user authentication single sign-on for ERP systems are supported:

- SAP ERP and Business Warehouse (BW)
- PeopleSoft Enterprise

3.1.8.1 Security plug-ins

Security plug-ins automate account creation and management by allowing you to map user accounts and groups from third-party systems into the BI platform. You can map third-party user accounts to existing Enterprise user accounts, or you can create new Enterprise user accounts that correspond to each mapped entry in the external system.

The security plug-ins dynamically maintain third-party user and group listings. So, once you map a Lightweight Directory Access Protocol (LDAP) or Windows Active Directory (AD) group to the BI platform, all users who belong to that group can log into the BI platform. Subsequent changes to the third-party group memberships are automatically propagated.

The BI platform supports the following security plug-ins:

- Enterprise security plug-in
  The Central Management Server (CMS) handles security information, such as user accounts, group memberships, and object rights that define user and group privileges. This is known as Enterprise authentication.
  Enterprise authentication is always enabled; it cannot be disabled. Use the system default Enterprise Authentication if you prefer to create distinct accounts and groups for use with the BI platform, or if you have not already set up a hierarchy of users and groups on an LDAP or Windows AD server.
  Trusted Authentication is a component of Enterprise authentication that integrates with third-party single sign-on solutions, including Java Authentication and Authorization Service (JAAS). Applications that have established trust with the Central Management Server can use Trusted Authentication to allow users to log on without providing their passwords.

- LDAP security plug-in
- Windows AD

> **Note**
>
> Although a user can configure Windows AD authentication for the BI platform and custom applications through the CMC, the CMC and BI launch pad do not support Windows AD authentication with NTLM. The only methods of authentication that the CMC and BI launch pad support are Windows AD with Kerberos, LDAP, Enterprise, and Trusted Authentication.

3.1.8.2 Enterprise Resource Planning (ERP) integration

An Enterprise Resource Planning (ERP) application supports the essential functions of an organization's processes by collecting real-time information related to day-to-day operations. The BI platform supports single sign-on and reporting from the following ERP systems:

- SAP ERP and Business Warehouse (BW)
- PeopleSoft Enterprise

> **Note**
>
> - SAP ERP and BW support is installed by default. Use the *Custom / Expand* installation option to deselect SAP integration support if you do not want support for SAP ERP or BW.
> - Support for PeopleSoft is not installed by default. Use the *Custom / Expand* installation option to select and install integration for non-SAP ERP systems.

For detailed information on the specific versions supported by the BI platform, consult the *Supported Platforms/PARs*, available at https://support.sap.com/home.html.

To configure ERP integration, see the *Supplementary Configurations for ERP Environments* chapter of this guide.

3.1.9 SAP Integration

The BI platform integrates with your existing SAP infrastructure with the following SAP tools:

- SAP System Landscape Directory (SLD)
  The system landscape directory of SAP NetWeaver is the central source of system landscape information relevant for the management of your software life cycle. By providing a directory comprising information about all installable software available from SAP and automatically updated data about systems already installed in a landscape, you get the foundation for tool support to plan software life-cycle tasks in your system landscape.
  The BI platform installation program registers the vendor and product names and versions with the SLD, as well as server and front-end component names, versions, and location.
- SAP Solution Manager
  The SAP Solution Manager is a platform that provides the integrated content, tools, and methodologies to implement, support, operate and monitor an organization's SAP and non-SAP solutions.

Non-SAP software with an SAP-certified integration is entered into a central repository and transferred automatically to your SAP System Landscape Directories (SLD). SAP customers can then easily identify which version of third-party product integration has been certified by SAP within their SAP system environment. This service provides additional awareness for third-party products besides our online catalogs for third-party products.
SAP Solution Manager is available to SAP customers at no extra charge, and includes direct access to SAP support and SAP product upgrade path information. For more information on SLD, see "Registration of the BI platform in the System Landscape".

- Monitoring with CA Wily Introscope
  CA Wily Introscope is a web application management product that delivers the ability to monitor and diagnose performance problems that may occur within Java-based SAP modules in production, including visibility into custom Java applications and connections to back-end systems. It allows you to isolate performance bottlenecks in NetWeaver modules including individual Servlets, JSPs, EJBs, JCOs, Classes, Methods and more. It offers real-time, low-overhead monitoring, end-to-end transaction visibility, historical data for analysis or capacity planning, customizable dashboards, automated threshold alarms, and an open architecture to extend monitoring beyond NetWeaver environments.

3.1.10 Integrated version control

The files that make up the BI platform on a server system are managed under version control. The installation includes options for version control systems such as Subversion and Git, but they are not configured by default. You can choose to set up one of these or integrate an existing version control system.

A version control system enables the storage and restoration of different revisions of configuration and other files, ensuring that the system can always be reverted to a known state from any point in the past.

3.2 Servers, services, nodes, and hosts

The BI platform uses the terms server and service to refer to the two types of software running on a BI platform computer.

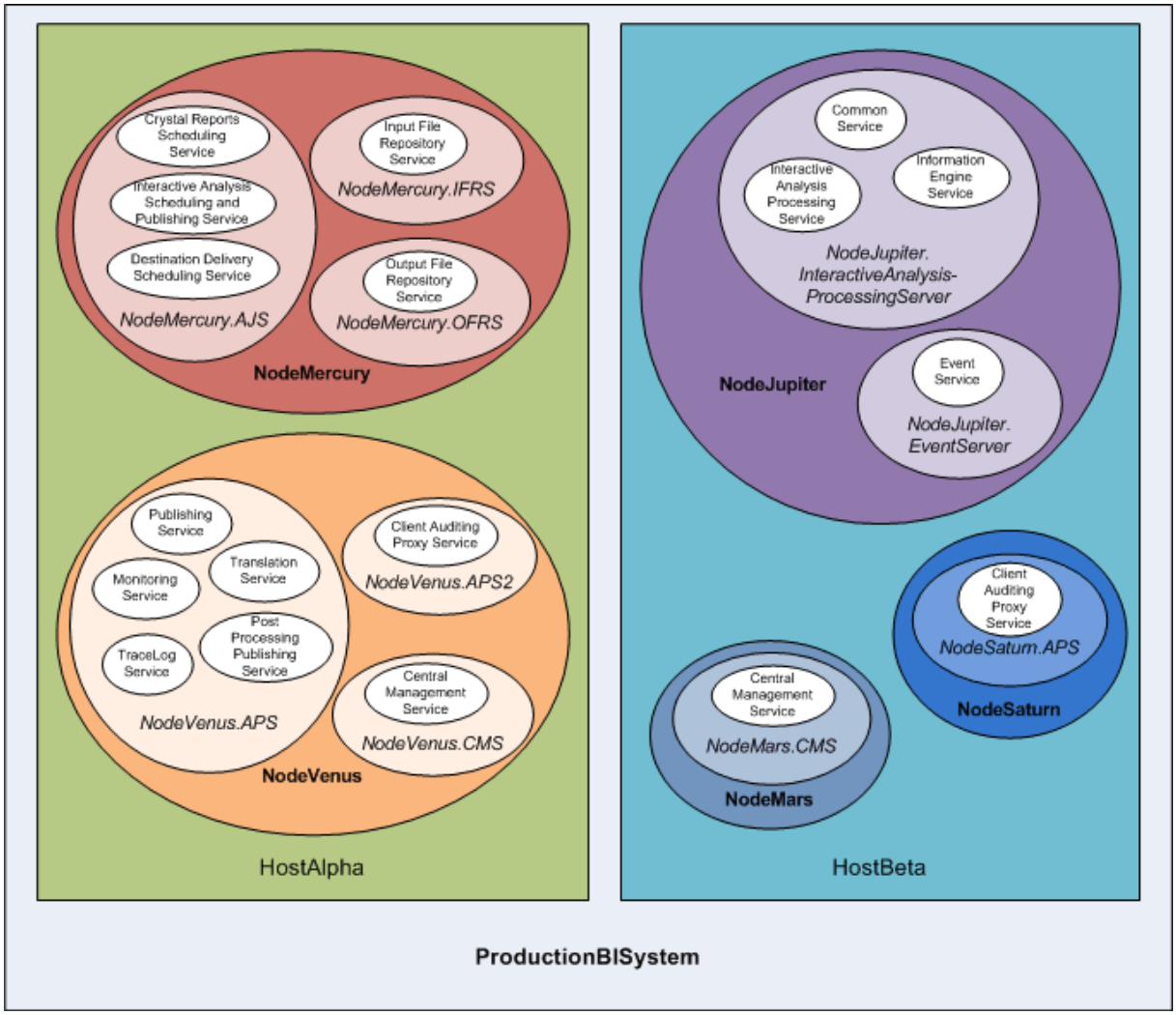
The term "server" is used to describe an operating-system-level process (on some systems, this is referred to as a daemon) that hosts one or more services. For example, the Central Management Server (CMS) and Adaptive Processing Server are servers. A server runs under a specific operating system account and has its own process ID (PID).

A service is a server subsystem that performs a specific function. The service runs within the memory space of its server under the process ID of the parent container (server). For example, the Web Intelligence Scheduling Service is a subsystem that runs within the Adaptive Job Server.

A node is a collection of BI platform servers running on the same host and managed by the same Server Intelligence Agent (SIA). One or more nodes can be on a single host.

The BI platform can be installed on a single computer, spread across different computers on an intranet, or separated over a wide area network (WAN).

The following diagram shows a hypothetical installation of the BI platform. The number of hosts, nodes, servers, and services—as well as the type of servers, and services—varies in actual installations.



Two hosts form the cluster named ProductionBISystem:

- The host named HostAlpha has the BI platform installed and is configured to have two nodes:
  - NodeMercury contains an Adaptive Job Server (`NodeMercury.AJS`) with services to schedule and publish reports, an Input File Repository Server (`NodeMercury.IFRS`) with a service to store input reports, and an Output File Repository Server (`NodeMercury.OFRS`) with a service to store report output.
  - NodeVenus contains an Adaptive Processing Server (`NodeVenus.APS`) with services to provide publishing, monitoring, and translation features, an Adaptive Processing Server (`NodeVenus.APS2`) with a service to provide client auditing, and a Central Management Server (`NodeVenus.CMS`) with a service to provide the CMS services.
- The host named HostBeta has the BI platform installed and is configured to have three nodes:
  - NodeMars contains a Central Management Server (`NodeMars.CMS`) with a service to provide the CMS services. Having the CMS on two computers enables load balancing and mitigation and failover capabilities.
  - NodeJupiter contains a Web Intelligence Processing Server (`NodeJupiter.Web Intelligence`) with a service to provide Web Intelligence reporting, and an Event Server (`NodeJupiter.EventServer`) to provide report monitoring of files.

- NodeSaturn contains an Adaptive Processing Server (`NodeSaturn.APS`) with a service to provide client auditing.

3.2.1 Server changes since XI 3.1

The following table describes major changes in the BI platform servers since XI 3.1. Types of changes include:

- Servers that have changed names between versions, while providing the same or similar functionality.
- Servers that are no longer offered by newer versions.
- Common or related services that have been consolidated onto the Adaptive servers.
  For example, the scheduling services provided by individual Job servers in XI 3.1 have been moved to the Adaptive Job Server since 4.0.
- New servers that have been introduced.

Server changes

XI 3.1	4.0	4.0 Feature Pack 3	4.1	4.2	4.3	BI2025 (4.4)
Connection Server [1]	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server
Crystal Reports Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Crystal Reports Processing Server	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2013 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2016 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2020 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2025 Processing Server
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (BI Workspaces)	Not available as of 4.0 Feature Pack 3	Not available in 4.1	Not available in 4.2	Not available in 4.3	Not available in 4.4
Dashboard Analytics Server (Dashboard Builder) [2]	Dashboard Analytics Server (BI Workspaces)	Not available as of 4.0 Feature Pack 3	Not available in 4.1	Not available in 4.2	Not available in 4.3	Not available in 4.4

XI 3.1	4.0	4.0 Feature Pack 3	4.1	4.2	4.3	BI2025 (4.4)
Desktop Intelligence Cache Server [3]	Not available as of 4.0	Not available as of 4.0	Not available in 4.1 [3]	Not available in 4.2 [3]	Not available in 4.3 [3]	Not available in 4.4
Desktop Intelligence Job Server [3]	Not available as of 4.0	Not available as of 4.0	Not available in 4.1 [3]	Not available in 4.2 [3]	Not available in 4.3 [3]	Not available in 4.4
Desktop Intelligence Processing Server [3]	Not available as of 4.0	Not available as of 4.0	Not available in 4.1 [3]	Not available in 4.2 [3]	Not available in 4.3 [3]	Not available in 4.4
Destination Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Multi-Dimensional Analysis Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server
Program Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2013 Report Application Server (RAS)	Crystal Reports 2016 Report Application Server (RAS)	Crystal Reports 2020 Report Application Server (RAS)	Crystal Reports 2025 Report Application Server (RAS)
Web Intelligence Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Xcelsius Cache Server [4]	Dashboard Design Cache Server (Xcelsius) [5]	Dashboards Cache Server (Xcelsius)	Dashboards Cache Server (Xcelsius)	Dashboards Cache Server (Xcelsius)	Not available in 4.3 [7]	Not available in 4.4
Xcelsius Processing Server [4]	Dashboard Design Processing Server (Xcelsius) [5]	Dashboards Processing Server (Xcelsius)	Dashboards Processing Server (Xcelsius)	Dashboards Processing Server (Xcelsius)	Not available in 4.3 [7]	Not available in 4.4
Content Specific web parts [6]	Crystal report viewer, Xcelsius viewer, and Analytical Report viewer	Crystal report viewer, Xcelsius viewer, and Analytical Report viewer	Crystal report viewer, Xcelsius viewer, and Analytical Report viewer	Crystal report viewer, Xcelsius viewer, and Analytical Report viewer	Content Specific web parts are deprecated in 4.3	Content Specific web parts are deprecated in 4.4

- [1] In 4.0, Connection Server 32 is 32-bit and runs connections specifically to data sources that do not support 64-bit middleware. Connection Server is 64-bit and runs connections to all other data sources. For more information, see the *Data Access Guide*.
- [2] The Dashboard Server and Dashboard Analytics Server have been removed in 4.0 Feature Pack 3. Server configuration is no longer required for BI workspace functionality (formerly Dashboard Builder in XI 3.1).

- [3] Desktop Intelligence was not available in version 4.0 and 4.0 maintenance packs. The Desktop Intelligence client application is available in version 4.1, but Desktop Intelligence servers are not. Desktop Intelligence reports can be converted to Web Intelligence documents using the Report Conversion Tool.
- [5] Dashboard Design servers in 4.0 have been renamed to “Dashboards” in 4.0 Feature Pack 3 to align with the product name change to SAP BusinessObjects Dashboards.
- [6] The following content specific web parts are deprecated in 4.3:
  - Crystal report viewer
  - Xcelsius viewer
  - Analytical Report viewer
- [7] Both Dashboards Processing Server (Xcelsius) and Dashboards Cache Server (Xcelsius) are deprecated.

3.2.2 Services

When adding servers, you must include some services on the Adaptive Job Server. For example, the Destination Delivery Scheduling Service.

> **Note**
>
> - New services or server types may be added in future maintenance releases.
> - The Sample Java Scheduling Service is consumed only for internal development purposes and is unavailable for consumption by external stakeholders.

Service	Service category	Server type	Service description
Adaptive Connectivity Service	Connectivity Services	Adaptive Processing Server	Provides connectivity services for Java-based drivers
Authentication Update Scheduling Service	Core Services	Adaptive Job Server	Provides synchronization of updates for third-party security plug-ins
Central Management Service	Core Services	Central Management Server	Provides server, user, session management, and security (access rights and authentication) management. At least one Central Management Service must be available in a cluster for the cluster to operate.
Client Auditing Proxy Service	Core Services	Adaptive Processing Server	Collects auditing events sent from clients and forwards them to the CMS server
Commentary Service	Core Services	Adaptive Processing Server	Allows commenting operations in documents.

Service	Service category	Server type	Service description
Crystal Reports 2025 Processing Service	Crystal Reports Services	Crystal Reports Processing Server	Accepts and processes Crystal Reports 2025 reports; can share data between reports to reduce the number of database accesses
Crystal Reports 2025 Scheduling Service	Crystal Reports Services	Adaptive Job Server	Runs scheduled legacy Crystal Reports jobs and publishes the results to an output location
Crystal Reports 2025 Viewing and Modification Service	Crystal Reports Services	Report Application Server (RAS)	Processes viewing and modification requests for Crystal Reports 2025 reports.
Crystal Reports Cache Service	Crystal Reports Services	Crystal Reports Cache Server	Limits the number of database accesses generated from Crystal reports and speeds up reporting by managing a cache of reports
Crystal Reports DSL Engine Service	Crystal Reports Services	Adaptive Processing Server	Provides Dimensional Semantic Layer (DSL) services to Crystal Reports 202x
Custom Data Access Service	Web Intelligence Services	Adaptive Processing Server	Provides dynamic connections to data sources that do not require a Connection Server. This service allows accessing and refreshing reports created using some personal data providers, such as CSV files. See the *SAP BusinessObjects Web Intelligence Rich Client User Guide* for more information on building a query or refreshing a document based on a text file.
Data Federation Service	Data Federation Services	Adaptive Processing Server	Queries and processes the underlying data sources for a multi-source universe

Service	Service category	Server type	Service description
Destination Delivery Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled jobs and publishes the results to an output location, such as a file system, FTP server, SFTP server, email, or a user's inbox **Note** When adding servers, you must include some Adaptive Job Server services—including this service.
Document Recovery Service	Web Intelligence Services	Adaptive Processing Server	Web Intelligence document auto-save and recovery
DSL Bridge Service	Web Intelligence Services	Adaptive Processing Server	Dimensional Semantic Layer (DSL) session support
Event Service	Core Services	Event Server	Monitors for file events on a File Repository Server (FRS) and triggers reports to run when required
Excel Data Access Service	Web Intelligence Services	Adaptive Processing Server	Supports Excel files uploaded to the BI platform as data sources. See *SAP BusinessObjects Web Intelligence Rich Client User Guide* for more information on building a query or refreshing a document based on an Excel file.
Information Engine Service	Web Intelligence Services	Web Intelligence Processing Server	Required service for Web Intelligence documents processing
Input Filestore Service	Core Services	Input File Repository Server	Maintains published report and program objects that can be used in the generation of new reports when an input file is received
Insight to Action Service	Core Services	Adaptive Processing Server	Enables actions to be invoked and provides support for RRI
Promotion Management ClearCase Service	Promotion Management Services	Adaptive Processing Server	Provides ClearCase support for LCM
Promotion Management Scheduling Service	Promotion Management Services	Adaptive Job Server	Runs scheduled Promotion Management jobs

Service	Service category	Server type	Service description
Promotion Management Service	Promotion Management Services	Adaptive Processing Server	Promotion Management Core service
Monitoring Service	Core Services	Adaptive Processing Server	Provides monitoring functions
Multi-Dimensional Analysis Service	Analysis Services	Adaptive Processing Server	Provides access to multidimensional Online Analytical Processing (OLAP) data; converts the raw data into XML, which can be rendered into Excel, PDF, or Analysis (formerly Voyager) crosstabs and charts
Native Connectivity Service	Connectivity Services	Connection Server	Provides Native Connectivity services for 64-bit architecture
Native Connectivity Service (32-bit)	Connectivity Services	Connection Server	Provides Native Connectivity services for 32-bit architecture
Output Filestore Service	Core Services	Output File Repository Server	Maintains a collection of completed documents
Platform Search Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled search to index all content in the Central Management Server (CMS) repository
Platform Search Service	Core Services	Adaptive Processing Server	Provides searching functionality for the BI platform
Probe Scheduling Service	Core Services	Adaptive Job Server	Provides scheduled Probe jobs and publishes the results to an output location
Program Scheduling Service	Core Services	Adaptive Job Server	Runs programs that have been scheduled to run at a given time
Publication Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled publishing jobs and publishes the results to an output location
Publishing Post Processing Service	Core Services	Adaptive Processing Server	Performs actions on reports after they have completed, such as sending a report to an output location

Service	Service category	Server type	Service description
Publishing Service	Core Services	Adaptive Processing Server	Coordinates with the Publishing Post Processing Service and Destination Job Service to publish reports to an output location, such as a file system, FTP server, SFTP server, email, or a user's inbox
Rebean Service	Web Intelligence Services	Adaptive Processing Server	SDK used by Web Intelligence and Explorer
Replication Service	Core Services	Adaptive Job Server	Runs scheduled federation jobs to replicate content between federated sites
Security Query Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled Security Query jobs
Security Token Service	Core Services	Adaptive Processing Server	SAP Single Sign-On support
Set Materialization Service	Core Services	Adaptive Processing Server	Operates materialization of sets and set groups.
Set Materialization Scheduling Service	Core Services	Adaptive Job Server	Allows scheduling of sets and set groups for materialization.
Translation Service	Core Services	Adaptive Processing Server	Translates InfoObjects with input from the Translation Manager client
Users and Groups Import Scheduling Service	Core Services	Adaptive Job Server	Allows scheduling of principal file imports
Visual Difference Scheduling Service	Promotion Management Services	Adaptive Job Server	Runs scheduled Visual Difference (Promotion Management) jobs and publishes the results to an output location
Visual Difference Service	Promotion Management Services	Adaptive Processing Server	Determines whether documents are visually identical for doc promotion and Promotion Management
Visualization Service	Web Intelligence Services	Adaptive Processing Server	A common Visualization Object Model Service used by Web Intelligence
Web Intelligence Common Service	Web Intelligence Services	Web Intelligence Processing Server	Supports Web Intelligence documents processing
Web Intelligence Core Service	Web Intelligence Services	Web Intelligence Processing Server	Supports Web Intelligence documents processing
Web Intelligence Processing Service	Web Intelligence Services	Web Intelligence Processing Server	Accepts and processes Web Intelligence documents

Service	Service category	Server type	Service description
Web Intelligence Scheduling Service	Web Intelligence Services	Adaptive Job Server	Enables support for scheduled Web Intelligence jobs
Version Management Service	Promotion Management Services	Adaptive Processing Server	Manages multiple versions of BI resources using IBM Rational ClearCase or Apache Subversion.

3.2.3 Service categories

> **Note**
>
> New services or server types may be added in future maintenance releases.

Service category	Service	Server type
Analysis Services	Multi-Dimensional Analysis Service	Adaptive Processing Server
Connectivity Services	Adaptive Connectivity Service	Adaptive Processing Server
Connectivity Services	Native Connectivity Service	Connection Server
Connectivity Services	Native Connectivity Service (32-bit)	Connection Server
Core Services	Authentication Update Scheduling Service	Adaptive Job Server
Core Services	Central Management Service	Central Management Server
Core Services	Client Auditing Proxy Service	Adaptive Processing Server
Core Services	Commentary Service	Adaptive Processing Server
Core Services	Destination Configuration Service*	Adaptive Job Server
Core Services	Destination Delivery Scheduling Service	Adaptive Job Server
Core Services	Event Service	Event Server
Core Services	Insight to Action Service	Adaptive Processing Server
Core Services	Input Filestore Service	Input File Repository Server
Core Services	Monitoring Service	Adaptive Processing Server
Core Services	Output Filestore Service	Output File Repository Server
Core Services	Platform Search Scheduling Service	Adaptive Job Server
Core Services	Platform Search Service	Adaptive Processing Server
Core Services	Probe Scheduling Service	Adaptive Job Server
Core Services	Program Scheduling Service	Adaptive Job Server
Core Services	Publication Scheduling Service	Adaptive Job Server
Core Services	Publishing Post Processing Service	Adaptive Processing Server

Service category	Service	Server type
Core Services	Publishing Service	Adaptive Processing Server
Core Services	Replication Service	Adaptive Job Server
Core Services	Security Query Scheduling Service	Adaptive Job Server
Core Services	Security Token Service	Adaptive Processing Server
Core Services	Set Materialization Service	Adaptive Processing Server
Core Services	Set Materialization Scheduling Service	Adaptive Processing Server
Core Services	Single Sign-on Service*	Central Management Server, Connection Server, Crystal Reports Processing Server, RAS, and Web Intelligence Processing Server
Core Services	TraceLog Service*	Any server
Core Services	Translation Service	Adaptive Processing Server
Core Services	Users and Groups Import Scheduling Service*	Adaptive Job Server
Crystal Reports Services	Crystal Reports 2025 Processing Service	Crystal Reports Processing Server
Crystal Reports Services	Crystal Reports 2025 Scheduling Service	Adaptive Job Server
Crystal Reports Services	Crystal Reports 2025 Viewing and Modification Service	Report Application Server (RAS)
Crystal Reports Services	Crystal Reports Cache Service	Crystal Reports Cache Server
Crystal Reports Services	Crystal Reports DSL Engine Service	Adaptive Processing Server
Data Federation Services	Data Federation Service	Adaptive Processing Server
Lifecycle Management Services	Promotion Management ClearCase Service	Adaptive Processing Server
Lifecycle Management Services	Promotion Management Scheduling Service	Adaptive Job Server
Lifecycle Management Services	Promotion Management Service	Adaptive Processing Server
Lifecycle Management Services	Visual Difference Scheduling Service	Adaptive Job Server
Lifecycle Management Services	Visual Difference Service	Adaptive Processing Server
Web Intelligence Services	Custom Data Access Service	Adaptive Processing Server
Web Intelligence Services	Document Recovery Service	Adaptive Processing Server
Web Intelligence Services	DSL Bridge Service	Adaptive Processing Server
Web Intelligence Services	Excel Data Access Service	Adaptive Processing Server
Web Intelligence Services	Information Engine Service	Web Intelligence Processing Server
Web Intelligence Services	Rebean Service	Adaptive Processing Server
Web Intelligence Services	Visualization Service	Adaptive Processing Server
Web Intelligence Services	Web Intelligence Common Service	Web Intelligence Processing Server

Service category	Service	Server type
Web Intelligence Services	Web Intelligence Core Service	Web Intelligence Processing Server
Web Intelligence Services	Web Intelligence Monitoring Service*	Adaptive Processing Server
Web Intelligence Services	Web Intelligence Processing Service	Web Intelligence Processing Server
Web Intelligence Services	Web Intelligence Scheduling Service	Adaptive Job Server
Promotion Management Services	Version Management Service	Adaptive Processing Server

3.2.4 Server types

An asterisk beside a service name indicates it is a secondary service. Some secondary services are created automatically, but you must choose to include other secondary services after selecting the primary service that a secondary service depends on.

> **Note**
>
> New services or server types may be added in future maintenance releases.

Server type	Service	Service category
Any server	TraceLog Service*	Core Services
Adaptive Job Server	Authentication Update Scheduling Service	Core Services
Adaptive Job Server	Crystal Reports 2025 Scheduling Service	Crystal Reports Services
Adaptive Job Server	Destination Configuration Service*	Core Services
Adaptive Job Server	Destination Delivery Scheduling Service	Core Services
Adaptive Job Server	Promotion Management Scheduling Service	Promotion Management Services
Adaptive Job Server	Platform Search Scheduling Service	Core Services
Adaptive Job Server	Probe Scheduling Service	Core Services
Adaptive Job Server	Program Scheduling Service	Core Services
Adaptive Job Server	Publication Scheduling Service	Core Services
Adaptive Job Server	Replication Service	Core Services
Adaptive Job Server	Security Query Scheduling Service	Core Services
Adaptive Job Server	Set Materialization Scheduling Services	Core services
Adaptive Job Server	Users and Groups Import Scheduling Service*	Core Services
Adaptive Job Server	Visual Difference Scheduling Service	Promotion Management Services
Adaptive Job Server	Web Intelligence Scheduling Service	Web Intelligence Services

Server type	Service	Service category
Adaptive Processing Server	Analytical Hub services	Core Services
Adaptive Processing Server	BEx Web Application Service	Analysis Services
Adaptive Processing Server	Client Auditing Proxy Service	Core Services
Adaptive Processing Server	Crystal Reports DSL Engine Service	Crystal Reports Services
Adaptive Processing Server	Custom Data Access Service	Web Intelligence Services
Adaptive Processing Server	Data Federation Service	Data Federation Services
Adaptive Processing Server	Document Recovery Service	Web Intelligence Services
Adaptive Processing Server	DSL Bridge Service	Web Intelligence Services
Adaptive Processing Server	Excel Data Access Service	Web Intelligence Services
Adaptive Processing Server	Insight to Action Service	Core Services
Adaptive Processing Server	Promotion Management ClearCase Service	Promotion Management Services
Adaptive Processing Server	Promotion Management Service	Promotion Management Services
Adaptive Processing Server	Monitoring Service	Core Services
Adaptive Processing Server	Multi-Dimensional Analysis Service	Analysis Services
Adaptive Processing Server	Platform Search Service	Core Services
Adaptive Processing Server	Publishing Post Processing Service	Core Services
Adaptive Processing Server	Publishing Service	Core Services
Adaptive Processing Server	Rebean Service	Web Intelligence Services
Adaptive Processing Server	Security Token Service	Core Services
Adaptive Processing Server	Set materialization Service	Core Services
Adaptive Processing Server	Translation Service	Core Services
Adaptive Processing Server	Visual Difference Service	Promotion Management Services
Adaptive Processing Server	Visualization Service	Web Intelligence Services
Adaptive Processing Server	Web Intelligence Monitoring Service*	Web Intelligence Services
Central Management Server	Central Management Service	Core Services
Central Management Server	Single Sign-on Service*	Core Services
Connection Server	Native Connectivity Service	Connectivity Services
Connection Server	Single Sign-on Service*	Core Services
Crystal Reports Cache Server	Crystal Reports Cache Service	Crystal Reports Services
Crystal Reports Processing Server	Single Sign-on Service*	Core Services
Event Server	Event Service	Core Services
Input File Repository Server	Input Filestore Service	Core Services
Output File Repository Server	Output Filestore Service	Core Services

Server type	Service	Service category
Report Application Server (RAS)	Crystal Reports 2025 Viewing and Modification Service	Crystal Reports Services
RAS	Single Sign-on Service*	Core Services
Web Intelligence Processing Server	Information Engine Service	Web Intelligence Services
Web Intelligence Processing Server	Single Sign-on Service*	Core Services
Web Intelligence Processing Server	Web Intelligence Common Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Core Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Processing Service	Web Intelligence Services

3.2.5 Servers

Servers are collections of services running under a Server Intelligence Agent (SIA) on a host. The type of server is denoted by the services running within it. Servers can be created in the Central Management Console (CMC). The following table lists the different types of servers that can be created in the CMC.

Server	Description
Adaptive Job Server	A generic server that processes scheduled jobs. When you add a Job server to the BI platform system, you can configure the Job server to process reports, documents, programs, or publications and send the results to different destinations.
Adaptive Processing Server	A generic server that hosts services responsible for processing requests from a variety of sources. The installation program installs one Adaptive Processing Server (APS) per host system. Depending on the features that you've installed, this APS may host a large number of services, such as the Monitoring Service, Lifecycle Management Service, Multi-Dimensional Analysis Service (MDAS), Publishing Service, and others. For production or test systems, the best practice is to create additional APSs, and configure the APSs to meet your business requirements. For more information, see Introduction to the System Configuration Wizard [page 76] and Configuring Adaptive Processing Servers for production systems [page 438].
Central Management Server (CMS)	Maintains a database of information about your BI platform system (in the CMS system database) and audited user actions (in the Auditing Data Store). All platform services are managed by the CMS. The CMS also controls access to the system files where documents are stored, and information on users, user groups, security levels (including authentication and authorization), and content.

Server	Description
Connection Server	Provides database access to source data. It supports relational databases, as well as OLAP and other formats. The Connection Server is responsible for handling connection and interaction with the various data sources and providing a common feature set to clients.
Crystal Reports Cache Server	Intercepts report requests sent from clients to the page server. If the cache server cannot fulfill the request with a cached report page, it passes the request on to the Crystal Reports Processing server, which runs the report and returns the results. The cache server then caches the report page for potential future use.
Crystal Reports Processing Server	Responds to page requests by processing reports and generating encapsulated page format (EPF) pages. The key benefit of EPF is that it supports page-on-demand access, so only the requested page is returned, not the entire report. This improves system performance and reduces unnecessary network traffic for large reports.
Event Server	Monitors the system for events, which can act as a trigger for running a report. When you set up an event trigger, the Event Server monitors the condition and notifies the CMS that an event has occurred. The CMS can then start any jobs that are set to run upon the event. The Event Server manages file-based events that occur in the storage tier.
File Repository Server	Responsible for the creation of file system objects, such as exported reports, and imported files in non-native formats. An Input FRS stores report and program objects that have been published to the system by administrators or end users. An Output FRS stores all of the report instances generated by the Job Server.
Web Intelligence Processing Server	Processes SAP BusinessObjects Web Intelligence documents.
Report Application Server	Provides ad-hoc reporting capabilities that allow users to create and modify Crystal reports via the SAP Crystal Reports Server Embedded Software Development Kit (SDK).

3.3 Client applications

You can interact with the BI platform using two main types of client applications:

- Desktop applications
  These applications must be installed on a supported Microsoft Windows operating system, and can process data and create reports locally.

> **Note**
>
> The BI platform installation program no longer installs desktop applications. To install desktop applications on a server, use the stand-alone SAP BusinessObjects Business Intelligence platform Client Tools installation program.

Desktop clients allow you to offload some BI report processing onto individual client computers. Most desktop applications directly access your organization's data through drivers installed on the desktop, and communicate with your BI platform deployment through CORBA or encrypted CORBA SSL.
An example of this type of application is Crystal Reports.

- Web applications
  These applications are hosted by a web application server and can be accessed with a supported web browser on Windows, Macintosh, Unix, and Linux operating systems.
  This allows you to provide business intelligence (BI) access to large groups of users, without the challenges of deploying desktop software products. Communication is conducted over HTTP, with or without SSL encryption (HTTPS).
  Examples of this type of application include BI launch pad, SAP BusinessObjects Web Intelligence, the Central Management Console (CMC), and report viewers.

3.3.1 Installed with SAP BusinessObjects Business Intelligence platform Client Tools

3.3.1.1 Web Intelligence Rich Client

Web Intelligence Rich Client is an ad-hoc analysis and reporting tool for business users with or without access to the BI platform.

It allows business users to access data via universes (.unx), SAP HANA, SAP Datasphere, or other sources, using familiar business terms in a drag-and-drop interface. Workflows allow very broad or very narrow questions to be analyzed, and for further questions to be asked at any point in the analysis workflow.

Web Intelligence Rich Client users can continue working with Web Intelligence document files (.wid) even when unable to connect to a Central Management Server (CMS).

It is no longer possible to install Web Intelligence Rich Client from the SAP BI Launch Pad by default. For more information, see .

> **Note**
>
> - We do not recommend installing Web Intelligence Rich Client on the same machine as the BI platform servers. Web Intelligence Rich Client and the BI Platform servers have binaries in common, which could cause issues to your deployment if you upgrade the installation (client or server). If you are installing Web Intelligence Rich Client, please install it on a separate machine.
> - If you're updating, make sure to stop and close existing version before installing the new version. Check the Windows system tray, the Rich Client might be minimized and is still running.

3.3.1.2 Business View Manager

Business View Manager allows users to build semantic layer objects that simplify underlying database complexity.

Business View Manager can create data connections, dynamic data connections, data foundations, business elements, business views, and relational views. It also allows detailed column and row-level security to be set for the objects in a report.

Designers can build connections to multiple data sources, join tables, alias field names, create calculated fields, and then use the simplified structure as a Business View. Report designers and users can then use the business view as the basis for their reports, rather than and building their own queries from the data directly.

3.3.1.3 Report Conversion Tool

RCT is deprecated in BI 4.3 release. For more details, please refer to **2801797**.

3.3.1.4 Universe Design Tool

Universe Design Tool is removed in BI 2025 release. For more details, please refer to 3520314.

3.3.1.5 Information Design Tool

Information Design Tool (formerly Information Designer) is a metadata design environment that enables a designer to extract, define, and manipulate metadata from relational and OLAP sources to create and deploy SAP BusinessObjects universes.

3.3.1.6 Translation Management Tool

The BI platform provides support for multilingual documents and universes. A multilingual document contains localized versions of universe metadata and document prompts. A user can create reports, for example, from the same universe in their chosen languages.

Translation Management Tool (formerly Translation Manager) defines the multilingual universes and manages translation of universes and other report and analytic resources in the CMS repository.

Translation Management Tool:

- Translates universe or documents for a multilingual audience.
- Defines the metadata language parts of a document, and the appropriate translation. It generates external XLIFF format and imports XLIFF files to get translated information.

- Lists the universe or document structure to be translated.
- Lets you translate the metadata through the user interface, or through an external translation tool by importing and exporting XLIFF files.
- Creates multilingual documents.

3.3.1.7 Data Federation Administration Tool

The Data Federation Administration Tool (formerly Data Federator) is a rich client application that offers easy-to-use features to manage your data federation service.

Tightly integrated in the BI platform, the data federation service enables multi-source universes by distributing queries across disparate data sources, and lets you federate data through a single data foundation.

The data federation administration tool lets you optimize data federation queries and fine-tune the data federation query engine for the best possible performance.

You use the data federation administration tool to do the following:

- Test SQL queries.
- Visualize optimization plans which detail how federated queries are distributed to each source.
- Compute statistics and set system parameters to fine-tune the data federation services and get the best possible performance.
- Manage properties to control how queries are executed in each data source at the connector level.
- Monitor running SQL queries.
- Browse the history of executed queries.

3.3.2 Installed with SAP BusinessObjects Business Intelligence platform

3.3.2.1 Central Configuration Manager (CCM)

The Central Configuration Manager (CCM) is a server troubleshooting and node management tool provided in two forms. In a Microsoft Windows environment, the CCM allows you to manage local and remote servers through its graphical user interface (GUI) or from a command line. In a Unix environment, the CCM shell script (`ccm.sh`) allows you to manage servers from the command line.

You use the CCM to create and configure nodes and to start or stop your web application server, if it is the default bundled Tomcat web application server. On Windows, it also allows you to configure network parameters, such as Secure Sockets Layer (SSL) encryption. These parameters apply to all servers within a node.

> **Note**
>
> Most server management tasks are now handled through the CMC, not through the CCM. The CCM is now used for troubleshooting and node configuration.

3.3.2.2 Upgrade Management Tool

UMT is being deprecated in BI 4.3 release. For more details, please refer to 2801797

3.3.2.3 Repository Diagnostic Tool

The Repository Diagnostic Tool (RDT) can scan, diagnose, and repair inconsistencies that may occur between the Central Management Server (CMS) system database and the File Repository Servers (FRS) filestore.

It can also report the repair status and completed actions. To determine synchronization between the file system and database, the RDT should be used after the user first completes a hot back-up. It can also be used after a restoration and prior to starting their BI platform services. The user can set a limit for the number of errors the RDT will find and repair before stopping.

3.3.3 Available separately

3.3.3.1 SAP BusinessObjects Analysis, edition for Microsoft Office

SAP BusinessObjects Analysis, edition for Microsoft Office is a premium alternative to Business Explorer (BEx) and allows business analysts to explore multi-dimensional online analytical processing (OLAP) data.

Analysts can quickly answer business questions and then share their analysis and workspace with others as *analyses*.

SAP BusinessObjects Analysis, edition for Microsoft Office enables analysts to:

- Discover trends, outliers, and details stored in financial systems without the help of a database administrator.
- Get answers to business questions while viewing large or small multi-dimensional data sets efficiently.
- Access the full range of OLAP data sources available within the organization and share results using a simple, intuitive interface.
- Access multiple different OLAP sources in the same analyses to get a comprehensive view of the business and the cross-impact that one trend may have on another.
- Interrogate, analyze, compare, and forecast business drivers.
- Use a comprehensive range of business and time calculations.

3.3.3.2 SAP Crystal Reports

SAP Crystal Reports software enables users to design interactive reports from a data source.

3.3.3.3 SAP Lumira

SAP Lumira application helps you to visualize data, and create stories about data. Using SAP Lumira, you can manipulate, edit, format, and refine your data, create visualizations to represent the data graphically, and share your visualizations using stories.

SAP Lumira is now listed as an application in CMC, which enables you to manage rights related to data acquisition and content sharing functionality of SAP Lumira for each user or user group.

> ⓘ Note
>
> All events related to the SAP Lumira application are registered without a client ID in the auditing database.

3.3.4 Web application clients

Web application clients reside on a web application server, and are accessed on a client web browser. Web applications are automatically deployed when you install the BI platform.

Web applications are easy for users to access from a web browser, and communication can be secured with SSL encryption if you plan to allow users access from outside your organization's network.

Java web applications can also be reconfigured or deployed after the initial installation by using the bundled WDeploy command-line tool, which allows you to deploy web applications to a web application server in two ways:

1. Standalone mode
   All web application resources are deployed to a web application server that serves both dynamic and static content. This arrangement is suitable for small installations.
2. Split mode
   The web application's static content (HTML, images, CSS) is deployed to a dedicated web server, while dynamic content (JSPs) is deployed to a web application server. This arrangement is suitable for larger installations that will benefit from the web application server being freed up from serving static web content.

For more information about WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

3.3.4.1 Central Management Console (CMC)

The Central Management Console (CMC) is a web-based tool that you use to perform administrative tasks (including user, content, and server management) and to configure security settings. Because the CMC is a web-based application, you can perform all of the administrative tasks in a web browser on any computer that can connect to the web application server.

Only members of the Administrators group can change management settings, unless a user is explicitly granted rights to do so. Roles can be assigned in the CMC to grant user privileges to perform minor

administrative tasks, such as managing users in your group and managing reports in folders that belong to your team.

3.3.4.2 Fiorified BI Launch Pad

Fiorified BI Launch Pad (formerly InfoView) is a web-based interface that end users access to view, schedule, and keep track of published business intelligence (BI) reports. Fiorified BI Launch Pad can access, interact with, and export, any type of business intelligence including reports, analytics, and dashboards.

Fiorified BI Launch Pad allows users to manage:

- BI content browsing and searching.
- BI content access (creating, editing, and viewing).
- BI content scheduling and publishing.

3.3.4.3 BI Workspaces

BI workspaces helps you track your business activities and performance using modules (templates for data) and Business Intelligence (BI) workspaces (viewing data in one or more modules). Modules and BI workspaces provide information needed to adjust business rules as conditions change. It helps you track and analyze key business data via management BI workspaces and modules. It also supports group decision-making and analysis via integrated collaboration and workflow capabilities. BI workspaces provides the following features:

- Tab-based browsing
- Page creation: Manage BI workspaces and modules
- A point and click application builder
- Content linking between modules for in-depth data analysis

> **Note**
>
> Content linking is not supported for Design Studio documents.

3.3.4.4 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence is a web-based tool that provides query, reporting, and analysis functionality for relational data sources in a single web-based product.

It allows users to create reports, perform ad-hoc queries, analyze data, and format reports in a drag-and-drop interface. Web Intelligence hides the complexity of underlying data sources.

Reports can be published to a supported web portal, or to Microsoft Office applications using SAP BusinessObjects Live Office.

3.4 Process Workflows

When tasks are performed such as logging in, scheduling a report, or viewing a report, information flows through the system and the servers communicate with each other. The following section describes some of the process flows as they would happen in the BI platform.

To view additional process workflows with visual aids, see the SAP BusinessObjects Business Intelligence 4.x platform Official Product Tutorials at: http://scn.sap.com/docs/DOC-8292

3.4.1 Startup and authentication

3.4.1.1 Logging on to the BI platform

Prerequisites

This workflow describes a user logging on to a BI platform web application from a web browser. This workflow applies to web applications such as BI launch pad and the Central Management Console (CMC).

Procedure

1. The browser (web client) sends the login request via the web server to the web application server, where the web application is running.
2. The web application server determines that the request is a logon request. The web application server sends the username, password, and authentication type to the CMS for authentication.
3. The CMS validates the username and password against the appropriate database. In this case, Enterprise authentication is used, and user credentials are authenticated against the CMS system database).
4. Upon successful validation, the CMS creates a session for the user in memory.
5. The CMS sends a response to the web application server to let it know that the validation was successful.
6. The web application server generates a logon token for the user session in memory. For the rest of this session, the web application server uses the logon token to validate the user against the CMS. The web application server generates the next web page to send to the web client.
7. The web application server sends the next web page to the web server.
8. The web server sends the web page to the web client where it is rendered in the user's browser.

3.4.1.2 SIA start-up

Context

A Server Intelligence Agent (SIA) can be configured to start automatically with the host operating system, or can be started manually with Central Configuration Manager (CCM).

A SIA retrieves information about the servers it manages from a Central Management Server (CMS). If the SIA uses a local CMS, and that CMS is not running, the SIA starts the CMS. If a SIA uses a remote CMS, it attempts to connect to the CMS.

Once a SIA is started, the following sequence of events is performed.

Procedure

1. The SIA looks in its cache to locate a CMS.
   a. If the SIA is configured to start a local CMS, and the CMS is not running, the SIA starts the CMS and connects.
   b. If the SIA is configured to use a running CMS (local or remote), it attempts to connect to the first CMS in its cache. If the CMS is not currently available, it attempts to connect to the next CMS in the cache. If none of the cached CMSs are available, the SIA waits for one to become available.
2. The CMS confirms the SIA's identity to ensure that it is valid.
3. Once the SIA has successfully connected to a CMS, it requests a list of servers to manage.

   > ⓘ Note
   >
   > A SIA does not store information about the servers it manages. The configuration information that dictates which server is managed by a SIA is stored in the CMS system database and is retrieved from the CMS by the SIA when it starts.

4. The CMS queries the CMS system database for a list of servers managed by the SIA. The configuration for each server is also retrieved.
5. The CMS returns the list of servers, and their configuration, to the SIA.
6. For each server configured to start automatically, the SIA starts it with the appropriate configuration and monitors its state. Each server started by the SIA is configured to use the same CMS used by the SIA.

   Any servers not configured to start automatically with the SIA will not start.

3.4.1.3 SIA shutdown

Context

The Server Intelligence Agent (SIA) automatically stops when you shut down the host operating system, or you can manually stop the SIA in the Central Configuration Manager (CCM).

When the SIA shuts down, the following steps are performed.

Procedure

The SIA tells the CMS that it is shutting down.

a. If the SIA is stopping because the host operating system is shutting down, the SIA requests its servers to stop. Servers that do not stop within 25 seconds are forcefully terminated.
b. If the SIA is being stopped manually, it will wait for the managed server to finish processing existing jobs. Managed servers will not accept any new jobs. Once all jobs are complete, the servers stop. Once all servers have stopped, the SIA stops too.

Results

During a forced shutdown, the SIA tells all managed servers to stop immediately.

3.4.2 Program objects

3.4.2.1 Setting a schedule for a program object

Prerequisites

This workflow describes how a user schedules a program object to run at a future time from a web application, such as the Central Management Console (CMC) or BI launch pad.

Procedure

1. The user sends the schedule request from the web client via the web server to the web application server.
2. The web application server interprets the request and determines that the request is a schedule request. The web application server sends the schedule time, database login values, parameter values, destination, and format to the specified Central Management Server (CMS).
3. The CMS ensures that the user has rights to schedule the object. If the user has sufficient rights, the CMS adds a new record to the CMS system database and adds the instance to its list of pending schedules.
4. The CMS sends a response that the schedule operation was successful to the web application server.
5. The web application server generates the next HTML page and sends it via the web server to the web client.

3.4.2.2 A scheduled program object runs

Prerequisites

This workflow describes the process of a scheduled program object running at a scheduled time.The Adaptive Job Server and Input File Repository Server must also be running.

> **Note**
>
> This workflow requires the CMS, Adaptive Job Server, and Input File Repository Server to be running.

Procedure

1. The Central Management Server (CMS) checks the CMS system database to determine if there is any scheduled SAP Crystal report to be run at that time.
2. When scheduled job time arrives, the CMS locates an available Program Scheduling Service running on an Adaptive Job Server. The CMS sends the job information to the Program Scheduling Service.
3. The Program Scheduling Service communicates with the Input File Repository Server (FRS) to obtain the program object.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.
4. The Program Scheduling Service launches the program.
5. The Program Scheduling Service updates the CMS periodically with the job status. The current status is Processing.
6. The Program Scheduling Service sends a log file to the Output FRS. The Output FRS notifies the Program Scheduling Service that the object was scheduled successfully by sending an object log file.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.
7. The Program Scheduling Service updates the CMS with the job status. The current status is Success.
8. The CMS updates the job status in its memory and then writes the instance information to the CMS system database.

3.4.3 Crystal Reports

3.4.3.1 Viewing a cached SAP Crystal report page

Prerequisites

This workflow describes the process of a user requesting a page in an SAP Crystal report (for example from the report viewer in BI launch pad), when the report page already exists on a cache server.

> **Note**
>
> This workflow requires the CMS and the Crystal Reports Cache Server to be running.

Procedure

1. The web client sends a view request in a URL via the web server to the web application server.
2. The web application server interprets the request and determines that it is a request to view a selected report page. The web application server sends a request to the Central Management Server (CMS) to ensure that the user has sufficient rights to view the report.
3. The CMS checks the CMS system database to verify the user has sufficient rights to view the report.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the report.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the page of the report (`.epf` file).
6. The Crystal Reports Cache Server checks to see if the requested `.epf` file exists in the cache directory. In this example, the `.epf` file is found.
7. The Crystal Reports Cache Server returns the requested page to the web application server.
8. The web application server sends the page to the web client via the web server, where the page is rendered and displayed.

3.4.3.2 Viewing a non-cached SAP Crystal Reports 2025 page

Prerequisites

This workflow describes the process of a user requesting a page in an SAP Crystal Reports 2025 report (for example from the report viewer in BI launch pad), when the page does not already exist on a cache server.

> **Note**
>
> This workflow requires the CMS, Crystal Reports Cache Server, Crystal Reports 2025 Processing Server, and Output File Repository Server to be running.

Procedure

1. The user sends the view request through the web server to the web application server.
2. The web application server interprets the request, determines that it is a request to view a selected report page, and sends a request to the Central Management Server (CMS) to ensure that the user has sufficient rights to view the report.
3. The CMS checks the CMS system database to verify the user has sufficient rights to view the report.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the report.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the page of the report (`.epf` file).
6. The Crystal Reports Cache Server determines if the requested file exists in the cache directory.
   In this example, the requested `.epf` file is not found in the cache directory.
7. The Crystal Reports Cache Server sends the request to the Crystal Reports 2025 Processing Server.
8. The Crystal Reports 2025 Processing Server queries the Output File Repository Server (FRS) for the requested report instance, and the Output FRS sends the requested report instance to the Crystal Reports 2025 Processing Server.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.

9. The Crystal Reports 2025 Processing Server opens the report instance and checks the report to determine if it has data.

   The Crystal Reports 2025 Processing Server determines that the report contains data, and creates the `.epf` file for the requested report page without having to connect to the production database.
10. The Crystal Reports 2025 Processing Server sends the `.epf` file to the Crystal Reports Cache Server.
11. The Crystal Reports Cache Server writes the `.epf` file to the cache directory.
12. The Crystal Reports Cache Server sends the requested page to the web application server.
13. The web application server sends the page to the web client via the web server, where the page is rendered and displayed.

3.4.3.3 Viewing an SAP Crystal Reports 2025 report on demand

Prerequisites

This workflow describes the process of a user requesting an SAP Crystal Reports 2025 report page on demand to see the latest data; for example, from the report viewer in BI launch pad.

> **Note**
>
> This workflow requires the CMS, Crystal Reports Cache Server, Crystal Reports 2025 Processing Server, and Input File Repository Server to be running.

Procedure

1. The user sends the view request through the web server to the web application server.
2. The web application server interprets the request and determines that it is a request to view a selected report page. The web application server sends a request to the Central Management Server (CMS) to ensure that the user has sufficient rights to view the report.
3. The CMS checks the CMS system database to verify the user has sufficient rights to view the report.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the report.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the page of the report (`.epf` file).
6. The Crystal Reports Cache Server checks to see if the page already exists. Unless the report meets the requirements for on demand report sharing (within a set time of another on demand request, database login, parameters), the Crystal Reports Cache Server sends a request for the Crystal Reports 2025 Processing Server to generate the page.
7. The Crystal Reports 2025 Processing Server requests the report object from the Input File Repository Server (FRS). The Input FRS streams a copy of the object to the Crystal Reports 2025 Processing Server.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.

8. The Crystal Reports 2025 Processing Server opens the report in its memory and checks to see if the report contains data. In this example, there is no data in the report object, so the Crystal Reports 2025 Processing Server connects to the data source to retrieve data and generate the report.
9. The Crystal Reports 2025 Processing Server sends the page (`.epf` file) to the Crystal Reports Cache Server. The Crystal Reports Cache Server stores a copy of the `.epf` file in its cache directory in anticipation of new viewing requests.
10. The Crystal Reports Cache Server sends the page to the web application server.
11. The web application server sends the page to the web client via the web server, where the page is rendered and displayed.

3.4.3.4 Setting a schedule for an SAP Crystal report

Prerequisites

This workflow describes the process of a user scheduling an SAP Crystal report to be run at a future time from a web application such as the Central Management Console (CMC) or BI launch pad.

Procedure

1. The web client submits a schedule request in a URL via the web server to the web application server.

2. The web application server interprets the URL request and determines that the request is a schedule request. The web application server sends the schedule time, database login values, parameter values, destination, and format to the specified Central Management Server (CMS).
3. The CMS ensures that the user has rights to schedule the object. If the user has sufficient rights, the CMS adds a new record to the CMS system database. The CMS also adds the instance to its list of pending schedules.
4. The CMS sends a response to the web application server to let it know that the schedule operation was successful.
5. The web application server generates the next HTML page and sends it via the web server to the web client.

3.4.3.5 A scheduled SAP Crystal Reports 2025 report runs

Prerequisites

This workflow describes the process of a scheduled SAP Crystal Reports 2025 report running at a scheduled time.

Procedure

1. The Central Management Server (CMS) checks the CMS system database to determine if there is any scheduled SAP Crystal report to be run at that time.
2. When scheduled job time arrives, the CMS locates an available Crystal Reports 2025 Scheduling Service running on an Adaptive Job Server (based on the *Maximum Jobs Allowed* value configured on each Adaptive Job Server). The CMS sends the job information (report ID, format, destination, logon information, parameters, and selection formulas) to the Crystal Reports 2025 Scheduling Service.
3. The Crystal Reports 2025 Scheduling Service communicates with the Input File Repository Server (FRS) to obtain a report template as per the requested report ID.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.

4. The Crystal Reports 2025 Scheduling Service starts the JobChildserver process.
5. The child process (JobChildserver) starts `ProcReport.dll` when it receives the template from the Input File Repository Server. `ProcReport.dll` contains all of the parameters that were passed from the CMS to the Crystal Reports 2025 Scheduling Service.
6. `ProcReport.dll` starts `crpe32.dll`, which processes the report according to the parameters passed.
7. While `crpe32.dll` is still processing the report, records are retrieved from the data source as defined in the report.
8. The Crystal Reports 2025 Scheduling Service updates the CMS periodically with the job status. The current status is Processing.
9. Once the report is compiled into the memory of the Crystal Reports 2025 Scheduling Service, it may be exported to a different format, such as Portable Document Format (PDF). When exporting to PDF, `crxfpdf.dll` is used.

10. The report with saved data is submitted to the scheduled location (such as email), and then it is sent to the Output FRS.

    > **Note**
    >
    > This step also requires communication with the CMS to locate the required server and objects.

11. The Crystal Reports 2025 Scheduling Service updates the CMS with the job status. The current status is Success.
12. The CMS updates the job status in its memory and then writes the instance information to the CMS system database.

3.4.4 Web Intelligence

3.4.4.1 Viewing an SAP BusinessObjects Web Intelligence document on demand

Prerequisites

This workflow describes the process of a user viewing an SAP BusinessObjects Web Intelligence document on demand to see the latest data; for example, from the Web Intelligence viewer in BI launch pad.

Procedure

1. A web browser sends the view request to the web application server via the web server.
2. The web application server interprets the request and determines that it is a request to view a Web Intelligence document. The web application server sends a request to the Central Management Server (CMS) to ensure that the user has sufficient rights to view the document.
3. The CMS checks the CMS system database to verify the user has sufficient rights to view the document.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the document.
5. The web application server sends a request to the Web Intelligence Processing Server, requesting the document.
6. The Web Intelligence Processing Server requests the document from the Input File Repository Server (FRS) as well as the universe file on which the requested document is built. The universe file contains metalayer information, including row-level and column-level security.
7. The Input FRS streams a copy of the document to the Web Intelligence Processing Server, as well as the universe file on which the requested document is built.

    > **Note**
    >
    > This step also requires communication with the CMS to locate the required server and objects.

8. The Web Intelligence Report Engine (on the Web Intelligence Processing Server) opens the document in memory and launches `QT.dll` and a Connection Server in process.
9. `QT.dll` generates, validates, and regenerates the SQL and connects to the database to run the query. The Connection Server uses the SQL to get the data from the database to the Report Engine where the document is processed.
10. The Web Intelligence Processing Server sends the viewable document page that was requested to the web application server.
11. The web application server sends the document page to the web client via the web server, where the page is rendered and displayed

3.4.4.2 Setting a schedule for an SAP BusinessObjects Web Intelligence document

Prerequisites

This workflow describes the process of a user scheduling an SAP BusinessObjects Web Intelligence document to be run at a future time from a web application such as the Central Management Console (CMC) or BI launch pad.

Procedure

1. The web client submits a schedule request in a URL via the web server to the web application server.
2. The web application server interprets the URL request and determines that the request is a schedule request. The web application server sends the schedule time, database login values, parameter values, destination, and format to the specified Central Management Server (CMS).
3. The CMS ensures that the user has rights to schedule the object. If the user has sufficient rights, the CMS adds a new record to the CMS system database. The CMS also adds the instance to its list of pending schedules.
4. The CMS sends a response to the web application server to let it know that the schedule operation was successful.
5. The web application server generates the next HTML page and sends it via the web server to the web client.

3.4.4.3 A scheduled SAP BusinessObjects Web Intelligence document runs

Prerequisites

This workflow describes the process of a scheduled SAP BusinessObjects Web Intelligence document running at a scheduled time.

Procedure

1. The Central Management Server (CMS) checks the CMS system database to determine if a Web Intelligence document is scheduled to run.
2. When the scheduled time arrives, the CMS locates an available Web Intelligence Scheduling Service running on an Adaptive Job Server. The CMS sends the schedule request and all information about the request to the Web Intelligence Scheduling Service.
3. The Web Intelligence Scheduling Service locates an available Web Intelligence Processing Server based on the *Maximum Connections* value configured on each Web Intelligence Processing Server.
4. The Web Intelligence Processing Server determines the location of the Input File Repository Server (FRS) that houses the document and the universe metalayer file on which the document is based. The Web Intelligence Processing Server then requests the document from the Input FRS. The Input FRS locates the Web Intelligence document as well as the universe file on which the document is based and then streams them to the Web Intelligence Processing Server.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.

5. The Web Intelligence document is placed in a temporary directory on the Web Intelligence Processing Server. The Web Intelligence Processing Server opens the document in memory, and `QT.dll` generates the SQL from the universe on which the document is based. The Connection Server libraries included in the Web Intelligence Processing Server connect to the data source. The query data passes through `QT.dll` back to the Report Engine in the Web Intelligence Processing Server, where the document is processed. A new successful instance is created.
6. The Web Intelligence Processing Server uploads the document instance to the Output FRS.

   > **Note**
   >
   > This step also requires communication with the CMS to locate the required server and objects.

7. The Web Intelligence Processing Server notifies the Web Intelligence Scheduling Service (on the Adaptive Job Server) that document creation is completed. If the document is scheduled to go to a destination (file system, FTP, SFTP, SMTP, or Inbox), the Adaptive Job Server retrieves the processed document from the Output FRS and delivers it to the specified destination(s). Assume that this is not the case in this example.
8. The Web Intelligence Scheduling Service updates the CMS with the job status.
9. The CMS updates the job status in its memory, and then writes the instance information to the CMS system database.

4 System Configuration Wizard

4.1 Introduction to the System Configuration Wizard

After you install SAP BusinessObjects Business Intelligence platform, you will likely want to perform essential post-installation configuration, such as choosing a deployment template, and selecting the SAP BusinessObjects products your organization will use. To perform this configuration, and to get the BI platform running in the shortest time possible, run the *System Configuration Wizard*.

Important benefits of using the wizard:

- The wizard explains and guides you through the configuration steps that you'll need to do.
- Using the wizard reduces the likelihood of system misconfiguration.
- The wizard configures settings for you, which speeds up system configuration.

By default, the wizard is set to run automatically when you log in to the Central Management Console (CMC), but you can also start the wizard from the *Manage* area in the CMC. You can rerun the wizard at any time to adjust your configuration, and you can always use the *Servers* management page in the CMC to fine-tune any settings, including the settings you made using the wizard.

> **Note**
>
> For improved security, only members of the Administrators group can access the wizard.

> **Note**
>
> To prevent the wizard from running automatically, the “Administrator” user can select the *Don't show this wizard when the CMC is started* check box on the first page of the wizard.

> **Note**
>
> If you plan to install any add-ons, or add nodes to your BI platform deployment, it is recommended that you perform those steps before running the System Configuration Wizard.

4.2 Specifying the products you use

You can simplify the configuration of BI platform servers by specifying the products your organization uses, and you can optimize resource allocation by stopping the servers for products your organization doesn't use. To do this, select products on the *Products* page. When you specify the products your organization uses, the wizard starts all servers and dependencies required for those products to run, and configures those servers and dependencies to start automatically whenever the BI platform starts. Also, by deselecting unused products, you can improve the start-up time and resource usage of the BI platform.

For example, if you select the Crystal Reports product, the BI platform will automatically start all Crystal Reports servers and appropriate dependencies.

To see a list of the servers that will be automatically started for a product, click the *?* icon beside the product's name.

The wizard configures product servers as follows:

- Selecting a product results in starting all servers belonging to that product, as well as other servers needed for that product to function (dependencies), when the wizard completes. Selecting a product also sets that product's servers to auto-start with the BI platform. If a server hosts services from multiple products, then if any of those products are selected, the server will be started. Note that some services from products that are not selected may be running if they are hosted by a server that also hosts services from products that are selected.
- Deselecting a product results in the servers used by that product being stopped, provided that those servers do not also host services from a product that is still selected, or services belonging to the Core Services category. The stopped product servers are set to not auto-start with the BI platform. If a server hosts services from both selected and deselected products, the server remains running.
- Deselecting a product may also result in stopping servers that don't belong to the deselected product, if there are dependent services used only by that deselected product. This will release resources because those dependent servers are not needed anymore.
- Deselecting products does not uninstall or remove files for those products.

Whenever you open the *Products* page, the product states on the page represent the current system state.

If all servers for a product are running, then the check box for that product is selected. If all servers for a product are stopped, then the check box is cleared. If only some servers for a product are running, while other servers are in other states, for example stopped, then the *Products* page displays the *Keep existing configuration* check box, to indicate that the system was configured outside of the wizard. You can clear the check box if you want to use the wizard to change your configuration.

> **Note**
>
> The *Products* page shows all products installed in the cluster. For example, if machine A has products P1 and P2 installed, and machine B has products P2 and P3 installed, then the *Products* page shows products P1, P2, and P3. Products that are not installed do not appear on the *Products* page.

> **Note**
>
> To simplify deployment, the configuration on this page does not need to be repeated for each node; instead, it is applied to the entire cluster.

> **Note**
>
> If any settings were previously modified in the CMC, the wizard displays a message informing you that the settings were changed outside of the wizard. You can choose to keep the existing configuration or override the current settings.

> **Note**
>
> Changes you make in the wizard are not applied until you click *Apply* on the *Review* page.

When you've finished making your changes, click *Next* to go to the next page of the wizard. You can also use the navigation panel at the left to jump directly to any page that you've already visited.

4.3 Choosing a deployment template

The default installation of the BI platform configures a small deployment that's suitable for a demo environment on limited system hardware. To better match your hardware and intended use case (for example, preparing a test system or production system), choose one of the predefined deployment templates from the *Capacity* page. These templates are intended to help you quickly get your BI platform system up and running, and shorten your initial deployment time.

Although choosing an appropriate deployment template helps with initial configuration and provides a good starting point, it is not a replacement for system sizing and tuning, which must still be performed. For best performance, you should size your system by referring to a sizing guide.

Choosing an appropriate deployment template is important for several reasons:

- The request-handling capacity of your system is affected by the deployment template you choose. A larger deployment provides greater capacity to handle more requests or more-complex requests. However, a larger deployment requires more system resources.
- Choosing a larger deployment does not guarantee better performance, particularly if you do not have sufficient available hardware resources.
- The deployment template you choose should match your business needs and your available hardware resources. The system may have reduced capacity and performance if you choose a deployment template that is too small for your business needs or too large for the available hardware resources.
- Larger deployment templates provide better compartmentalization: failures in one product are less likely to affect other products. Choose a template that balances resource (RAM) utilization and performance. For example, if a large amount of RAM is available, you may want to pick the biggest deployment template that your RAM permits; this will result in better system compartmentalization.

You can use the slider to select a deployment template, or you can choose a RAM amount from the drop-down list. As you change the setting, notice that the *Number of Adaptive Processing Servers* indicator changes to show you how your system will be configured if you choose that setting.

> **Note**
>
> The deployment template you choose affects only the Adaptive Processing Servers (APS). Other servers, for example the CMS, or Adaptive Job Servers, are not affected.

> **Note**
>
> RAM Required is the minimum amount of RAM required for BI platform servers. For example, on a machine with 16 GB of RAM, where the operating system uses 1 GB of RAM, the database server uses another 1 GB, and BI platform servers use 10 GB, RAM Required equals 10 GB, not 12 GB or 16 GB. The RAM Required number represents only a typical value; your system could need more RAM under heavy load. For optimal system performance, you should always perform system sizing.

> **Note**
>
> Whenever you open the *Capacity* page, the deployment template shown on the page represents the current system state, if the current system state matches one of the predefined deployment templates. For example, if you have manually created an extra Adaptive Processing Server using the CMC, the current state of your system doesn't match any of the deployment templates, so the *Capacity* page displays the *Keep existing configuration* check box to indicate that the system was configured outside of the wizard.

In a multi-node deployment, the *Keep existing configuration* check box is also displayed if any node has a number of APSs not matching a deployment template, or if the number of APSs on different nodes is different. You can clear the check box if you want to use the wizard to change your configuration.

> **Note**
>
> To simplify deployment, the APS configuration that you select is applied to each node (as long as those nodes have an APS installed), so the more nodes you have, the more capacity your cluster will have.

> **Note**
>
> Add-ons (for example, Data Services or Analysis Application Design Service (AADS)) are not managed by the wizard. Services created by the add-ons will not be moved to different APSs by the wizard.
>
> Examples:
>
> - If AADS is hosted by an APS that hosts other services from the main BI platform installation, then if you run the wizard and change the deployment template size from XS to M, the wizard creates seven new APSs and moves all services to the seven APSs, except for the AADS service, which remains in the initial APS.
> - The Data Services add-on creates a dedicated APS. The wizard does not alter this dedicated APS, and does not count this APS when it reports the number of APSs in the system.

The DeploymentTemplates.pdf file

For a detailed description of the settings that the wizard will make for each available deployment template, click the *deployment template* link on the *Capacity* page to open the `DeploymentTemplates.pdf` file.

The `DeploymentTemplates.pdf` file describes the deployment templates in detail. Note that the templates do not specify the number of users that can be supported; this is because the number of users that can be supported is dependent on load. You should perform system sizing to determine the number of users you'll need to support, and therefore the amount of RAM you'll need, the CPU requirements, and so on.

4.4 Specifying data folder locations

Use the *Folders* page to specify where you want the BI platform to save its data and log files. You can specify folder locations, or accept the current locations.

If your BI platform deployment has multiple nodes, you have two options for defining the folder locations:

- If you want to configure the same folder locations for all nodes, select the *All nodes have the same folder locations* option.
- If the servers in your cluster are not set up identically, the installation paths or file directory structures may be different. You can select the *Nodes have different folder locations* option to configure specific folder locations for each node.

Whenever the wizard opens to the *Folders* page, it displays the folder names as follows:

- If all nodes have folders with the exact same values (that is, the Log folders on all servers in the cluster are identical, and the Data folders on all servers in the cluster are identical, and so on), then the *All nodes have the same folder locations* option is selected and the current folder names are shown.
- If all folders of a particular type (Log, Data, Audit, Input File Store, or Output File Store) are identical within each node, but different between the nodes, then the *Nodes have different folder locations* option is selected and the current folder names are shown.
- If all folders of a particular type are not identical within each node, and different between the nodes, then the *Nodes have different folder locations* option is selected but the folder names are left blank.

If you are changing the locations of the folders, the wizard configures the system to use the new folders. With the exception of the auditing data folder, the wizard does not copy or move the contents of the original folders to the new folders. If the new folders do not already contain the correct content, or if you have data in the original folders and want to migrate it, you may want to move or copy that data to the new folders.

For the Input File Store, Output File Store, and Data folders, if the new folder location is empty, you should manually copy the files there from the old folder location, or restore files from a backup. For the Log folder, copy files from the old folder only if you want the new folder to contain the log files that exist at the old folder location.

> → Tip
>
> If you plan to copy or restore files to the new folders, do so before you restart the nodes.

Example scenarios:

- If you change a folder location, and the original folder contains reports, those reports won't be available in the BI platform until you copy them to the new folder and restart the nodes.
- If your original folder contained corrupted or modified reports, and you want to revert to a known-good backup, you would retrieve the reports from the backup and place them in the new folder, instead of copying the contents from the original folder.
- If your data files were originally located on a disk with drive letter X, and you change the drive letter to Y in the operating system, you don't need to copy or move the data files; you just need to change the folder location in the BI platform.

If you have manually changed some of the folder locations, so that some servers on a node use one set of folders, while other servers on the same node use different folders, the *Folders* page displays the *Keep existing configuration* check box to indicate that the system was configured outside of the wizard. For example, you may have two File Repository Servers from the same node configured to use different Log Folder paths. You can clear the check box if you want to use the wizard to change the current configuration.

For more information about the types of files stored in each folder, click the *?* icons.

> ⓘ Note
>
> If you change any of the following folder locations, you will need to manually restart all nodes after the wizard has completed for the changes to take effect:
>
> - Input File Store
> - Output File Store
> - Log Folder
> - Data Folder

4.5 Reviewing your changes

After you've finished choosing your configuration settings, they are displayed on the *Review* page for you to review, before the changes are applied to your BI platform system. For each category of settings, you can click *Details* to see a detailed description or listing of the settings and the changes that will be applied.

If you want to change any of the settings, you can access the individual pages directly from the navigation menu at the left side of the wizard.

Your selections are saved to a log file, which you can download from the Completed page.

A response file is also generated and saved. The response file helps you to automate system configuration. You can click the *Download* button to view the response file or download it to a local disk.

When you click *Apply*, your configuration settings are applied to your BI platform deployment. When the wizard completes, a *Completed* page is displayed, showing the next steps that you should perform manually.

Related Information

Log files and response files [page 81]

4.6 Log files and response files

The *Completed* page shows you the status of your changes, and lets you download and view the log and response files for your session.

The log and response files are saved automatically to the System Configuration Wizard folder, which you can access from the CMC. The file names are timestamped in the format `year_month_day_hour_minute_second`. Log files use a `.log` extension, while response files use an `.ini` extension.

You can also click the *Download* buttons to view the log and response files, or download them to a local disk.

The log file contains the following content:

- A record of all changes you made in this configuration session.
- The location where the response file is saved.
- A list describing the next steps you need to follow.

Related Information

Using a response file [page 82]

4.6.1 Using a response file

Each time the wizard completes, it saves a response file, containing your selections or answers (responses) to all the questions on the wizard's pages. The response file can be used to configure other clusters in your BI platform deployment without having to step through the wizard for each one, or it can be used at a later date if you want to set the system to the same configuration state. Using a response file lets you automate your deployment and avoid operator errors.

To use a response file, you run a script that takes the response file as a parameter. First, locate the response file that you want to use, and save it to disk. Response files are saved automatically to the System Configuration Wizard folder, which administrators can access from the CMC. The file names are timestamped in the format `year_month_day_hour_minute_second` and have an `.ini` extension. From the CMC, you can view the response file and save it to disk, or use the menu commands *Organize* > *Send* > *File Location*.

You can also download the response file for your current wizard session from the *Review* or *Completed* page, and save it to disk.

If you want to modify the settings in the response file before using it, you can edit the response file in a text editor. See the sample response file below for details.

Running the script

Once you have the appropriate response file, use the file as a command-line parameter for the scripts that execute the wizard:

- On Windows, run the batch file `SCW.bat`.
- On Unix, run the script file `scw.sh`.

The batch and script files are located in the same folder where other server management scripts are located:

- On Windows: `<installdir>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.
- On Unix: `<installdir>/sap_bobj/enterprise_xi40/linux_x64/scripts`.

The batch and script files take these command-line parameters:

- `-help`: Display the command-line help.
- `-r`: Specify the path and name of the response file.
- `-cms`: Specify the Central Management Server (CMS) that you want to log in to. If this parameter is omitted, the CMS defaults to the local machine and the default port (6400). Example: `machine_name:6500`
- `-username`: Specify an account that provides administrative rights to the BI platform. If this parameter is omitted, the default Administrator account is used.
- `-password`: Specify the password for the account. If not specified, a blank password is attempted. To use the `-password` parameter, you must also use the `-username` parameter.

Examples

On Windows: `SCW.bat –r c:\folder\filename.ini –cms cmsname:6400 –username "administrator" –password samplepassword`

On Unix: `./scw.sh –r /home/folder/filename.ini –cms cmsname:6400 –username "administrator" –password samplepassword`

Sample response file

```
# ******************************************
# ***************** Products *****************
# ******************************************
# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the
“Products.” settings below.
Products.KeepExistingConfiguration = true
# The “Products.” settings below will be ignored if
Products.KeepExistingConfiguration = true.
# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI
platform.
# "false": the product's servers are not auto-started with BI platform.
# Crystal Reports
Products.crystalreports = true
# Web Intelligence
Products.webintelligence = false
# Dashboards (Xcelsius)
Products.dashboards = false
# Data Federator
Products.datafederator = true
# Lifecycle Manager
Products.LCM = true
# ******************************************************
# ***************** Deployment Template *****************
# ******************************************************
# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and
the Capacity.DeploymentTemplate setting below will be ignored.
# "false": the deployment template configuration will be modified according to
the Capacity.DeploymentTemplate setting below.
Capacity.KeepExistingConfiguration = true
# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.
Capacity.DeploymentTemplate = xs
# ******************************************
# ***************** Folders ****************
# ******************************************
# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders."
settings below.
Folders.KeepExistingConfiguration = true
# The “Folders.” settings below will be ignored if
Folders.KeepExistingConfiguration = true.
# ------ All nodes use the same folders ------
```

```
# Use this section when you have one node, or when all nodes have the same
folder locations. Otherwise, comment it out.
Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>
# ------ Nodes use different folders ------
# Use this section when nodes have different folder locations. Otherwise,
comment it out.
# ------ NodeOne ------
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>
# ------ NodeTwo ------
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

All settings in the response file must be specified, and none of the settings can be empty, except in these cases:

- If you have a multi-node deployment, you can choose to omit the folder settings for one or more nodes, which will leave the folders on those nodes unchanged. However, for the nodes that you do specify in the response file, all folder locations must be specified.
- If the `KeepExistingConfiguration` parameter is set to `true`, you can omit the remaining settings for that page. For example, if `Products.KeepExistingConfiguration = true`, you can omit the remaining *Products* settings from the response file.

In some cases, the response file will include different products than the products that are installed in your target cluster. In those cases, these behaviors apply:

- If the response file doesn't contain definitions for products that are installed in the target cluster, the operation will fail.
- If the response file contains definitions for products that are not present in the target cluster, a warning message is added to the log file, and the remaining products will be properly configured.

> **Note**
>
> After you use a response file to configure a cluster, you will need to manually perform the additional steps described in the "Next steps" section of the log file.

> **Note**
>
> For increased security, only Enterprise authentication support is required (not Windows AD, LDAP, or SAP).

> **Note**
>
> If you prefer to postpone the restart of any nodes to the next scheduled restart, run the script just before a scheduled system down time.

5 Managing Licenses

5.1 Managing license keys

This section describes how to manage license keys for your BI platform deployment.

Related Information

To view license information [page 85]
To add a license key [page 86]
To view current account activity [page 87]

5.1.1 To view license information

Context

The *License Keys* management area of the CMC identifies the number of concurrent, named, and processor licenses that are associated with each key.

Procedure

1. Go to the *License Keys* management area of the CMC.
2. Select a license key.

   The details associated with the key appear in the *License Key Information* area. To purchase additional license keys, contact your SAP sales representative.

Related Information

To add a license key [page 86]
To view current account activity [page 87]

5.1.2 To add a license key

Prerequisites

If you are upgrading from a trial version of the product, be sure to delete the Evaluation key prior to adding any new license keys or product activation keycodes. After adding the new license keys, you will need to enable all your servers again.

> **Note**
>
> If you have received new license keys following a change in the way your organization implements BI platform licenses, you must delete all previous license keys from the system to maintain compliance.

> **Note**
>
> When you update to SAP BusinessObjects Business Intelligence Platform 4.2 Support Package 2 or a higher version from any lower versions, the existing licenses behave as expired licenses. You need to generate a new license key for SAP BusinessObjects Business Intelligence Platform 4.2, and use it.

Procedure

1. Go to the *License Keys* management area of the CMC.
2. Type the key in the *Add Key* field.
3. Click *Add*.

Results

The key is added to the list.

Related Information

To view license information [page 85]
To view current account activity [page 87]

5.1.3 To view current account activity

Procedure

1. Go to the *Settings* management area of the CMC.
2. Click *View global system metrics*.

   This section displays current license usage, along with additional job metrics.

Related Information

To add a license key [page 86]
To view license information [page 85]

6 Managing Users and Groups

6.1 Account management overview

Account management involves all of the tasks related to creating, mapping, changing, and organizing user and group information. The *Users and Groups* management area of the Central Management Console (CMC) provides a central place to perform these tasks.

After the user accounts and groups have been created, you can add objects and specify rights to them. When the users log on, they can view the objects using BI launch pad or their custom web application.

6.1.1 User management

In the *Users and Groups* management area, you can specify everything required for a user to access the BI platform. You can also view the two default user accounts summarized by the "Default user accounts" table.

Default user accounts

Account name	Description
Administrator	This user belongs to the *Administrators* and *Everyone* groups. An administrator can perform all tasks in all BI platform applications (for example, the CMC, CCM, Publishing Wizard, and BI launch pad).
Guest	This user belongs to the *Everyone* group. This account is enabled by default, and is not assigned a password by the system. If you assign it a password, the single sign-on to BI launch pad will be broken.
SMAdmin	This is a read-only account used by SAP Solution Manager to access BI platform components.

> **Note**
>
> Object migrations are best performed by members of the Administrators group, in particular the Administrator user account. To migrate an object, many related objects may also need to be migrated. Obtaining the required security rights for all the objects may not be possible for a delegated administrator account.

6.1.2 Group management

Groups are collections of users who share the same account privileges; therefore, you may create groups that are based on department, role, or location. Groups enable you to change the rights for users in one place (a

group) instead of modifying the rights for each user account individually. Also, you can assign object rights to a group or groups.

In the *Users and Groups* area, you can create groups that give a number of people access to the report or folder. This enables you to make changes in one place instead of modifying each user account individually. You can also view the several default group accounts summarized by the "Default group accounts" table.

To view available groups in the CMC, click *Group List* in the *Tree* panel. Alternatively, you can click *Group Hierarchy* to display a hierarchal list of all available groups.

Default group accounts

Account name	Description
Administrators	Members of this group can perform all tasks in all of the BI platform applications (CMC, CCM, Publishing Wizard, and BI launch pad). By default, the *Administrators* group contains only the Administrator user.
Everyone	Each user is a member of the *Everyone* group.
Translators	Members of this group have access to the Translation Manager application.

Related Information

How rights work in BI platform [page 115]
Granting access to users and groups [page 102]

6.1.3 Available authentication types

Before setting up user accounts and groups within the BI platform, decide which type of authentication you want to use. The "Authentication types" table summarizes the authentication options, which may be available to you, depending on the security tools your organization uses.

Authentication types

Authentication type	Description
Enterprise	Use the system default Enterprise Authentication if you prefer to create distinct accounts and groups for use with BI platform, or if you have not already set up a hierarchy of users and groups in an LDAP directory server, or a Windows AD server.
LDAP	If you set up an LDAP directory server, you can use existing LDAP user accounts and groups in the BI platform. When you map LDAP accounts to the BI platform, users are able to access BI platform applications with their LDAP user name and password. This eliminates the need to recreate individual user and group accounts within the BI platform.

Authentication type	Description
Windows AD	You can use existing Windows AD user accounts and groups in the BI platform. When you map AD accounts to the BI platform, users are able to log on to BI platform applications with their AD user name and password. This eliminates the need to recreate individual user and group accounts within the BI platform.
SAP	You can map existing SAP roles into BI platform accounts. After you map SAP roles, users are able to log on to BI platform applications with their SAP credentials. This eliminates the need to recreate individual user and group accounts within the BI platform.
PeopleSoft Enterprise	You can map existing PeopleSoft roles into BI platform accounts. After you map PeopleSoft roles, users are able to log on to BI platform applications with their PeopleSoft credentials. This eliminates the need to recreate individual user and group accounts within the BI platform.

6.2 Managing Enterprise and general accounts

Since Enterprise authentication is the default authentication method for the BI platform, it is automatically enabled when you first install the system. When you add and manage users and groups, the BI platform maintains the user and group information within its database.

> **Note**
>
> When a user logs off a web session on the BI platform by navigating to a non-platform page or closing the web browser, the Enterprise session is not logged off and the user still holds a license. The Enterprise session will time out after approximately 24 hours. To end the user's Enterprise session and free the license for use by others, the user must log out of the BI platform.

6.2.1 To create a user account

When you create a new user, you specify the user's properties and select the group or groups for the user.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Click *Manage* > *New* > *New User*.
   The *New User* dialog box appears.

3. To create an Enterprise user:
   a. In the *Authentication Type* list, select *Enterprise*.
   b. Type the account name, full name, email, and description information.

      > → Tip
      >
      > Use the description area to include extra information about the user or account.

   c. Specify the password information and settings adhering to the password criteria defined for Enterprise Authentication.
4. To create a user that will logon using a different authentication type, select the appropriate option from the *Authentication Type* list, and type the account name.
5. Perform one of the following actions to designate the user account (based on your BI platform license agreement):
   - Select *Concurrent User* if this user belongs to a license agreement that stipulates the number of users allowed to connect at one time.
   - Select *Named User* if this user belongs to a license agreement that associates a specific user with a license. Named user licenses are useful for people who require access to the BI platform, regardless of how many other people are connected.

     > ⓘ Note
     >
     > Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in.
     >
     > However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

6. Click *Create & Close*.

   The user is added to the system and is automatically added to the Everyone group. An inbox is automatically created for the user, with an Enterprise alias.

Next Steps

You can now add the user to a group or specify rights for the user.

6.2.2 To modify a user account

Context

Use this procedure to modify a user's properties or group membership.

> **Note**
>
> The user will be affected if he or she is logged on when you are making the change.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user whose properties you want to change.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box for the user appears.
4. Modify the properties for the user.

   In addition to all of the options that were available when you initially created the account, you now can disable the account by selecting the *Account is disabled* check box.

   > **Note**
   >
   > Any changes you make to the user account do not appear until the next time the user logs on.
5. Click *Save & Close*.

Related Information

To create a new alias for an existing user [page 111]

6.2.3 To delete a user account

Context

Use this procedure to delete a user's account. The user might receive an error if they are logged on when their account is deleted. When you delete a user account, the Favorites folder, personal categories, and inbox for that user are deleted as well.

If you think the user might require access to the account again in the future, select the *Account is disabled* check box in the *Properties* dialog box of the selected user instead of deleting the account.

> **Note**
>
> Deleting a user account won't necessarily prevent the user from being able to log on to the BI platform again. If the user account also exists in a third-party system, and if the account belongs to a third-party group that is mapped to the BI platform, the user may still be able to log on.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user you want to delete.
3. Click *Manage* > *Delete*.

   The delete confirmation dialog box appears, notifying you if the selected user is the owner of one or more objects.
4. Choose *OK*.
   The user account is deleted.

Related Information

To modify a user account [page 91]
To disable an alias [page 113]

6.2.4 To create a new group

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Click *Manage* > *New* > *New Group*.
   The *Create New User Group* dialog box appears.
3. Enter the group name and description.
4. Click *OK*.

Next Steps

After creating a new group, you can add users, add subgroups, or specify group membership so that the new group is actually a subgroup. Because subgroups provide you with additional levels of organization, they are useful when you set object rights to control users' access to your BI platform content.

6.2.5 To modify a group's properties

Context

You can modify a group's properties by making changes to any of the settings.

> **Note**
>
> The users who belong to the group will be affected by the modification the next time they log on.

Procedure

1. In the *Users and Groups* management area of the CMC, select the group.
2. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
3. Modify the properties for the group.
   Click the links from the navigation list to access different dialog boxes and modify different properties.
   - If you want to change the title or description for the group, click *Properties*.
   - If you want to modify the rights that principals have to the group, click *User Security*.
   - If you want to modify profile values for group members, click *Profile Values*.
   - If you want to add the group as a subgroup to another group, click *Member Of*.
4. Click *Save*.

6.2.6 To view group members

Context

You can use this procedure to view the users who belong to a specific group.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Expand *Group Hierarchy* in the *Tree* panel.
3. Select the group in the *Tree* panel.

   > **Note**
   >
   > It may take a few minutes for your list to display if you have a large number of users in the group or if your group is mapped to a third-party directory.

   The list of users who belong to the group is displayed.

6.2.7 To add subgroups

Context

You can add a group to another group. When you do this, the group that you added becomes a subgroup.

> **Note**
>
> Adding a subgroup is similar to specifying group membership.

Procedure

1. In the *Users and Groups* management area of the CMC, select the group that you want to add as a subgroup to another group.
2. Click *Actions* > *Join Group*.
   The *Join Group* dialog box appears.
3. Move the group that you want to add the first group to from the *Available Groups* list to the *Destination Group(s)* list.
4. Click *OK*.

Related Information

To specify group membership [page 95]

6.2.8 To specify group membership

Context

You can make a group a member of another group. The group that becomes a member is referred to as a subgroup. The group that you add the subgroup to is the parent group. A subgroup inherits the rights of the parent group.

Procedure

1. In the *Users and Groups* management area of the CMC, click the group that you want to add to another group.

2. Click *Actions* > *Member Of*.
   The *Member Of* dialog box appears.
3. Click *Join Group*.
   The *Join Group* dialog box appears.
4. Move the group that you want to add the first group to from the *Available Groups* to the *Destination Group(s)* list.

   Any rights associated with the parent group will be inherited by the new group you have created.
5. Click *OK*.
   You return to the *Member Of* dialog box, and the parent group appears in the parent groups list.

6.2.9 To delete a group

Context

You can delete a group when that group is no longer required. You cannot delete the default groups Administrator and Everyone.

> **Note**
>
> The users who belong to the deleted group will be affected by the change the next time they log on.

> **Note**
>
> The users who belong to the deleted group will lose any rights they inherited from the group.

To delete a third-party authentication group, such as the Windows AD Users group, use the *Authentication* management area in CMC.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the group you want to delete.
3. Click *Manage* > *Delete*.
   The delete confirmation dialog box appears.
4. Click *OK*.
   The group is deleted.

6.2.10 To add users or user groups in bulk

Context

You can use a CSV (comma-separated values) file to add users or user groups in bulk to the CMC. In a correctly formatted CSV file, commas separate data in a line, as shown in the following example:

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

The following conditions apply to the bulk addition process:

- Any line in the CSV file that contains an error will be omitted from the import process.
- User accounts are initially disabled after being imported.
- You can use blank passwords when creating new users. However, you must use a valid Enterprise authentication password for subsequent updates to existing users.
- When a DBCredential is added to an account, database credentials will be enabled in the user's profile.

> **Note**
>
> Only users who are part of the default Administrators group can add users in bulk. This feature is not supported for delegated admins.

Procedure

1. In the *Users and Groups* management area of the CMC, select *Manage* > *Import* > *User/Group/DBCredential*.

   The *Import User/Group/DBCredential* dialog box appears.
2. Click *Browse*, select a CSV file, and click *Verify*.

   The file is processed. If data are formatted correctly in the file, the *Import* button becomes active. If data are not formatted correctly, information about the error appears, and you must resolve the error before the CMC can verify the file for import.
3. Click *Import*.

Results

The users or user groups are imported to the CMC.

Next Steps

To review users or user groups that you have added, select *Manage* > *Import* > *History* in the *Users and Groups* management area.

6.2.11 To enable the Guest account

Context

The Guest account is disabled by default to ensure that no one can log on to the BI platform with this account. This default setting also disables the anonymous single sign-on functionality of the BI platform, so users will be unable to access BI launch pad without providing a valid user name and password.

Perform this task if you want to enable the Guest account so that users do not require their own accounts to access BI launch pad.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Click *User List* on the navigation panel.
3. Select *Guest*.
4. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
5. Clear the *Account is disabled* check box.
6. Click *Save & Close*.

6.2.12 Adding users to groups

User groups enable administrators to perform BI launch pad tasks for batches of users (for example, you can customize preferences or schedule publications for particular user groups).

You can add users to groups in the following ways:

- Select the group, and click *Actions* > *Add Members to Group*.
- Select the user, and click *Actions* > *Member Of*.
- Select the user, and click *Actions* > *Join Group*.

You can add a user to more than one user group. However, when a user belongs to two or more user groups, BI launch pad displays preferences for only one group.

Related Information

To specify group membership [page 95]

6.2.12.1 Adding a user to one or more user groups

You can add a user to more than one user group. However, BI launch pad will display preferences for only one of the user groups.

Context

Procedure

1. In the *Users and Groups* management area of the CMC, select the user to add to a group.
2. Select *Actions* > *Join Group*.

   > **Note**
   >
   > All BI platform users of the system are part of the Everyone group.

3. In the *Join Group* dialog box, move the group to add the user to from the *Available Groups* list to the *Destination Group(s)* list.

   > **→ Tip**
   >
   > Use `SHIFT`+`click` or `CTRL`+`click` to select multiple groups.

4. Click *OK*.

6.2.12.2 Adding one or more users to a user group

You can add multiple users to a user group.

Context

Preferences set for a user group apply to all users in the group. BI launch pad displays preferences for one user group at a time.

Procedure

1. In the *Users and Groups* management area of the CMC, select the user group.
2. Select *Actions* > *Add Members to Group*.
3. In the *Add* dialog box, click *User list*.
   The *Available users/groups* list refreshes and displays all user accounts in the system.
4. Move one or more users to the group from the *Available users/groups* list to the *Selected users/groups* list.

   > → Tip
   >
   > To select multiple users, use `SHIFT`+`click` or `CTRL`+`click`. To search for a specific user, enter the user name in the *search* box.

   > → Tip
   >
   > If your system has a large number of users, click the *Previous* and *Next* buttons to navigate the list of users.
5. Click *OK*.

6.2.13 Changing password settings

Within the CMC, you can change the password settings for a specific user or for all users in the system. The various restrictions listed below apply only to Enterprise accounts—that is, the restrictions do not apply to accounts that you have mapped to an external user database (LDAP or Windows AD). Generally, however, your external system will enable you to place similar restrictions on the external accounts.

6.2.13.1 To change user password settings

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user whose password settings you want to change.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Select or clear the check box associated with the password setting you want to change.

   The available options are:

   - *Password never expires*
   - *User must change password at next logon*
   - *User cannot change password*
5. Click *Save & Close*.

> **Note**
>
> When you change a user's password, the user will be logged out of all existing sessions and directed to the home page to log in again.

6.2.13.2 To change general password settings

Context

> **Note**
>
> Inactive user accounts will not be automatically de-activated.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Enterprise*.
   The *Enterprise* dialog box appears.
3. Select the check box for each password setting that you want to use, and provide a value if necessary.

   The following table identifies the minimum and maximum values for each of the settings you can configure.

   Password settings

Password setting	Default	Minimum	Recommended Maximum
Must contain at least N Characters	8 characters	6 characters	255 characters
Must not exceed N characters	255 characters	13 characters	255 characters
Must change password every N day(s)	30 days	2 days	100 days
Cannot reuse the N most recent password(s)	3 passwords	1 password	100 passwords
Must wait N minute(s) to change password	0 minutes	0 minutes	100 minutes
Disable account after N failed attempts to log on	10 failed	1 failed	100 failed

Password setting	Default	Minimum	Recommended Maximum
Reset failed logon count after N minute(s)	5 minutes	1 minute	100 minutes
Re-enable account after N minute(s)	5 minutes	0 minutes	100 minutes

> **Note**
>
> When you upgrade from a lower version of SAP BusinessObjects Business Intelligence Platform to any higher version, or try to perform any kind of expand installation, you must set *Disable account after N failed attempts to log on* to the default value.

> **Note**
>
> The rules mentioned above are applicable only to Enterprise users and not for any other third-party authentication types.

4. Click *Update*.

6.2.14 Granting access to users and groups

You can grant users and groups administrative access to other users and groups. Administrative rights include: viewing, editing, and deleting objects; viewing and deleting object instances; and pausing object instances. For example, for troubleshooting and system maintenance, you may want to grant your IT department access to edit and delete objects.

Related Information

To assign principals to an access control list for an object [page 125]

6.2.15 Controlling access to user inboxes

When you add a user, the system automatically creates an inbox for that user. The inbox has the same name as the user. By default, only the user and the administrator have the right to access a user's inbox.

Related Information

Managing security settings for objects in the CMC [page 123]

6.2.16 Configuring Fiorified BI launch pad options

In the CMC, administrators can configure the Fiorified BI launch pad preferences for user groups.

> **Note**
>
> If a user belongs to two or more user groups, the Fiorified BI launch pad displays the preferences configured for only one group.

6.2.16.1 Configuring the Fiorified BI launch pad logon screen

By default, the Fiorified BI launch pad logon screen prompts users for their user name and password. You can also prompt the users for the CMS name and the authentication type. To change this setting, you need to edit the Fiorified BI launch pad properties for the BOE.war file.

6.2.16.1.1 To configure the Fiorified BI launch pad logon screen

Context

To modify Fiorified BI launch pad default settings, you need to set custom properties for the BOE.war file. This file is deployed on the machine hosting your web application server.

Procedure

1. Go to the following directory in your BI platform installation:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Create a new file using a text editor.
3. Save the file under the following name:

   `FioriBI.properties`
4. To include the authentication options on the Fiorified BI launch pad logon screen, add the following line:

   ```
   authentication.visible=true
   ```
5. To change the default authentication, add the following line:

   ```
   authentication.default=<authentication>
   ```

   Replace `<authentication>` with any of the following options:

Authentication type	<authentication> value
Enterprise	`secEnterprise`
LDAP	`secLDAP`
Windows AD	`secWinAD`
SAP	`secSAPR3`

6. To prompt users for the CMS name on the Fiorified BI launch pad logon screen, add the following line:

```
cms.visible=true
```

7. Save and close the file.
8. Restart your web application server.

Next Steps

Use WDeploy to redeploy the `BOE.war` file on the web application server. For more information on using WDeploy see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

6.2.16.2 Setting Fiorified BI Launch pad preferences for user groups in the CMC

Administrators configure the default Fiori BI Launch pad preferences for user groups in the CMC.

Administrator-configured preferences for a user group apply to all users in the group. If a user belongs to two or more user groups, the Fiorified BI Launch pad displays the preferences configured for only one group.

Users can configure their own preferences in the Fiorified BI Launch pad, and their preferences take precedence over the default values. They can also switch back to the default preferences at any given time. Refer to the *Setting Page Preferences* section for the *Fiorified Business Intelligence Launch Pad User Guide*.

However, if the administrator modifies the default Fiorified BI Launch pad preferences in the CMC, the default values take precedence over the user-defined values.

6.2.16.2.1 Setting Fiorified BI Launch pad preferences for a user group

Procedure

1. Go to the *Users and Groups management* area of the CMC.
2. Under *Group List*, select the user group for which to set the Fiorified BI Launch pad preferences.

3. Right-click and choose *Fiori BI Launch Pad Preferences*.
4. Clear the *No Preferences Defined* check box.
5. To customize the *Home* tab, perform one of the following actions to choose the desired home page on the tab:

Home page tab option	Action
Display the default Fiori BI Launch pad home tab	Choose *Default Home tab*
Display a specific home tab	Choose *Select Home tab*, then: 1. In the *Landing Page* field, select a landing page: • *My Home* • *Schedule* • *Inbox* • *Folders* • *Recycle Bin* 2. In the *List Documents As* field, choose *Tile view (Default)* or *List view*. 3. In the *Landing Filter* field, select a landing filter: • *Show All* • *My Documents* • *All Categories* • *My Favorites* • *My Recently Viewed* • *My Recently Run* You can choose an object from *My Folders*, *Public Folders*, *Personal Categories*, and *Corporate Categories* to view it as the default landing page.
Display a specific report as home page	Choose *Select Report*, then click *Browse Documents* to choose a document from *My Folders* or *Public Folders*.
Display a category as home page	Choose *Select Category*, then click *Browse Categories* to choose a category from *Personal Categories* or *Corporate Categories*.

6. In the *Choose Column to display on Documents Tab* field, select the column preferences :
   - *Type*
   - *Last Run*
   - *Instances*
   - *Description*
   - *Created By*
   - *Last Updated*
   - *Created On*
   - *Location (Categories)*
   - *My Favorites (Home Page)*

- *Status (Schedule)*
- *Instance time (Schedule)*
- *Folder Path*

> **Note**
>
> The *Type*, *Description*, *Last Updated*, *My Favorites (Home page)*, *Status (Schedule)*, and *Instance time (Schedule)* columns are selected by default. You can modify the selection of columns you want to display.

7. Select *Save & Close*.

Next Steps

For the preferences defined by an administrator to be reflected in the interface, users must log onto the Fiorified BI Launch pad, choose *Settings* > *Account Preferences* > *Page Preferences*, and enable *Use Administrator Provided Settings*.

6.2.17 Managing attributes for system users

BI platform administrators define and add user attributes to system users through the *User Attribute Management* area in the Central Management Console (CMC). You can manage and extend attributes for the following user directories:

- Enterprise
- SAP
- LDAP
- Windows AD

When users are imported from external directories such as SAP, LDAP, and Windows AD, the following attributes are generally available for the user accounts:

- Full Name
- Email address

Attribute names

All user attributes added to the system must have the following properties:

- *Name*
- *Internal name*

The “Name” property is the friendly identifier for the attribute and it is used to query filters when working with the Universe semantic layer. For more information, see the *Information Design Tool* documentation. The

“Internal Name” is used by developers working with the BI platform SDK. This property is an automatically generated name.

Attribute names should not exceed 256 characters and should only contain alphanumeric characters and underscores.

> → Tip
>
> If you specify invalid characters for the Name attribute, the BI platform will not generate an internal name. Internal names cannot be modified once they are added to the system. It is recommended that you carefully select appropriate attribute names containing alphanumeric characters and underscores.

Prerequisites for expanding mapped user attributes

Before adding user attributes to the system, all relevant authentication plugins for the external user directories need to be configured to map and import users. In addition, you will need to be familiar with the schema of the external directories, in particular the names used for the target attributes.

> ⓘ Note
>
> For the SAP authentication plugin, only attributes contained in the BAPIADDR3 structure can be specified.

Once the BI platform is configured to map the new user attributes, values will be populated after the next scheduled update. All user attributes are displayed in the *User and Groups* management area of the CMC.

6.2.18 Prioritizing user attributes across multiple authentication options

When configuring SAP, LDAP, and AD authentication plugins, you can specify the priority levels for each plugin in relation to the other two. For example, in the LDAP authentication area use the *Set priority of LDAP attribute binding relative to other attributes binding* option to specify the LDAP priority in relation to SAP and AD. By default, the Enterprise attribute value takes priority over any value from an external directory. Attribute binding priorities are set at the authentication plugin level and not for any specific attribute.

Related Information

To configure the LDAP host [page 261]
To import SAP roles [page 332]

6.2.19 To add a new user attribute

Prerequisites

Before adding new user attribute to the BI platform, you must configure the authentication plugin for the external directory from which you are mapping user accounts. This applies to SAP, LDAP, and Windows AD. Specifically, you must check the *Import Full Name, Email Address and other attributes* option for all the required plugins.

> ⓘ Note
>
> You do not need to perform any preliminary tasks before expending attributes for Enterprise user accounts.

> → Tip
>
> If you plan to extend the same attribute across several plugins, it is recommended that you set the appropriate attribute binding priority level based on your organization's requirements.

Procedure

1. Go to the *User Attribute Management* management area of the CMC.
2. Click the *Add a New Custom Mapped Attribute* icon.
   The *Add Attribute* dialog box appears.
3. Specify a name for the new attribute in the *Name* field.

   The BI platform will use the name provided as a friendly name for the new attribute.

   As you enter the friendly name, the *Internal Name* field is automatically populated according to the following format: `SI_[Friendlyname]`. As the system administrator specifies a "friendly" attribute name, the BI platform automatically generates the "internal" name.
4. If necessary, modify the *Internal Name* field using letters, numerals or underscores.

   > → Tip
   >
   > The *Internal Name* field value can only be modified at this stage. You cannot edit this value once you have saved the new attribute.

   If the new attribute is for Enterprise accounts, skip to step 8.
5. Choose the appropriate option for *Add a new source for* from the list and click the *Add* icon. The following options are available:

   - *SAP*
   - *LDAP*
   - *AD*

   A table row is created for the attribute specified attribute source.
6. Specify under the *Attribute Source Name* column, the name of the attribute in the source directory.

   The BI platform does not provide a mechanism to automatically verify that the attribute name provided exists in the external directory. Ensure that the name provided is correct and valid.

7. Repeat steps 5-6 if additional sources are required for the new attribute.
8. Click *OK* to save and submit the new attribute to the BI platform.
   The new attribute Name, Internal Name, Source, and Attribute Source Name appear in the *User Attribute Management* management area of the CMC.

Results

The new attribute and its corresponding value for each affected user account. will be displayed upon the next scheduled refresh in the *Users and Groups* management area.

Next Steps

If you are using multiple sources for the new attribute, ensure that the correct attribute binding priorities are specified for each authentication plugin.

6.2.20 To edit customized user attributes

Context

Use the following procedure to edit user attributes that have been created in the BI platform. You can edit the following:

- The name of the attribute in the BI platform

  > **Note**
  >
  > This is not the Internal Name used for the attribute. Once an attribute is created and added to the BI platform, the internal name cannot be modified. To remove an internal name, administrators need to delete the associated attribute.

- The attribute source name
- Additional sources for the attribute

Procedure

1. Go to the *User Attribute Management* management area of the CMC.
2. Select the attribute you want to edit.
3. Click the *Edit selected attribute* icon.
   The *Edit* dialog box appears.

4. Modify the attribute Name or source information.
5. Click *OK* to save and submit the modifications to the BI platform.
   The modified values appear in the *User Attribute Management* management area of the CMC.

Results

The modified attribute name and values will appear after next scheduled refresh in the *Users and Groups* management area.

6.3 Managing aliases

If a user has multiple accounts in the BI platform, you can link the accounts using the Assign Alias feature. This is useful when a user has a third-party account that is mapped to Enterprise and an Enterprise account.

By assigning an alias to the user, the user can log on using either a third-party user name and password or an Enterprise user name and password. Thus, an alias enables a user to log on via more than one authentication type.

In the CMC, the alias information is displayed at the bottom of the *Properties* dialog box for a user. A user can have any combination of Enterprise, LDAP or Windows AD aliases.

6.3.1 To create a user and add a third-party alias

Context

When you create a user and select an authentication type other than Enterprise, the system creates the new user in the BI platform and creates a third-party alias for the user.

> ⓘ Note
>
> For the system to create the third-party alias, the following criteria must be met:
>
> - The authentication tool needs to have been enabled in the CMC.
> - The format of the account name must agree with the format required for the authentication type.
> - The user account must exist in the third-party authentication tool, and it must belong to a group that is already mapped to the BI platform.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Click *Manage* > *New* > *New User*.
   The *New User* dialog box appears.
3. Select the authentication type for the user, for example, Windows AD.
4. Type in the third-party account name for the user, for example, **`bsmith`**.
5. Select the connection type for the user.
6. Click *Create & Close*.

   The user is added to the BI platform and is assigned an alias for the authentication type you selected, for example, secWindowsAD:ENTERPRISE:bsmith. If required, you can add, assign, and reassign aliases to users.

6.3.2 To create a new alias for an existing user

Context

You can create aliases for existing BI platform users. The alias can be an Enterprise alias, or an alias for a third-party authentication tool.

> **Note**
>
> For the system to create the third-party alias, the following criteria must be met:
>
> - The authentication tool needs to have been enabled in the CMC.
> - The format of the account name must agree with the format required for the authentication type.
> - The user account must exist in the third-party authentication tool, and it must belong to a group that is mapped to the platform.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user that you want to add an alias to.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Click *New Alias*.
5. Select the authentication type.
6. Type in the account name for the user.
7. Click *Update*.

   An alias is created for the user. When you view the user in the CMC, at least two aliases are shown, the one that was already assigned to the user and the one you just created.

8. Click *Save & Close* to exit the *Properties* dialog box.

6.3.3 To assign an alias from another user

Context

When you assign an alias to a user, you move a third-party alias from another user to the user you are currently viewing. You cannot assign or reassign Enterprise aliases.

> **Note**
>
> If a user has only one alias and you assign that last alias to another user, the system will delete the user account, and the Favorites folder, personal categories, and inbox for that account.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user you want to assign an alias to.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Click *Assign Alias*.
5. Enter the user account that has the alias you want to assign, and click *Find Now*.
6. Move the alias you want to assign from the *Available aliases* list to the *Aliases to be added to* `<Username>` list.

   Here `<Username>` represents the name of the user you are assigning an alias to.

   > **→ Tip**
   >
   > To select multiple aliases, use the `SHIFT` + `click` or `CTRL` + `click` combination.
7. Click *OK*.

6.3.4 To delete an alias

When you delete an alias, the alias is removed from the system. If a user has only one alias and you delete that alias, the system automatically deletes the user account and the Favorites folder, personal categories, and inbox for that account.

Context

> **Note**
>
> Deleting a user's alias does not necessarily prevent the user from being able to log on to the BI platform again. If the user account still exists in the third-party system, and if the account belongs to a group that is mapped to the BI platform, then the BI platform will still allow the user to log on. Whether the system creates a new user or assigns the alias to an existing user, depends on which update options you have selected for the authentication tool in the *Authentication* management area of CMC.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user whose alias you want to delete.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Click the *Delete Alias* button next to the alias that you want to delete.
5. If prompted for confirmation, click *OK*.
   The alias is deleted.
6. Click *Save & Close* to exit the *Properties* dialog box.

6.3.5 To disable an alias

Context

You can prevent a user from logging on to the BI platform using a particular authentication method by disabling the user's alias associated with that method. To prevent a user from accessing the platform altogether, disable all aliases for that user.

> **Note**
>
> Deleting a user from the system does not necessarily prevent the user from being able to log on to the BI platform again. If the user account still exists in the third-party system, and if the account belongs to a group that is mapped to the platform, then the system will still allow the user to log on. To ensure a user can no longer use one of his or her aliases to log on to the platform, it is best to disable the alias.

Procedure

1. Go to the *Users and Groups* management area of the CMC.
2. Select the user whose alias you want to disable.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Clear the *Enabled* check box for the alias you want disable.

   Repeat this step for each alias you want to disable.
5. Click *Save & Close*.
   The user can no longer log on using the type of authentication that you just disabled.

Related Information

To delete an alias [page 113]

7 Setting Rights

7.1 How rights work in BI platform

Rights are the base units for controlling user access to the objects, users, applications, servers, and other features in the BI platform. They play an important role in securing the system by specifying the individual actions that users can perform on objects. Besides allowing you to control access to your BI platform content, rights enable you to delegate user and group management to different departments, and to provide your IT people with administrative access to servers and server groups.

It is important to note that rights are set on objects such as reports and folders rather than on the principals (the users and groups) who access them. For example, to give a manager access to a particular folder, in the *Folders* area, you add the manager to the access control list (the list of principals who have access to an object) for the folder. You cannot give the manager access by configuring the manager's rights settings in the *Users and Groups* area. The rights settings for the manager in the *Users and Groups* area are used to grant other principals (such as delegated administrators) access to the manager as an object in the system. In this way, principals are themselves like objects for others with greater rights to manage.

Each right on an object can be granted, denied, or unspecified. The BI platform security model is designed such that, if a right is left unspecified, the right is denied. Additionally, if settings result in a right being both granted and denied to a user or group, the right is denied. This "denial-based" design helps ensure that users and groups do not automatically acquire rights that are not explicitly granted.

There is an important exception to this rule. If a right is explicitly set on a child object that contradicts the rights inherited from the parent object, the right set on the child object overrides the inherited rights. This exception applies to users who are members of groups as well. If a user is explicitly granted a right that the user's group is denied, the right set on the user overrides the inherited rights.

Related Information

Rights override [page 119]

7.1.1 Access levels

Access levels are groups of rights that users frequently need. They allow administrators to set common security levels quickly and uniformly rather than requiring that individual rights be set one by one.

The BI platform comes with several predefined access levels. These predefined access levels are based on a model of increasing rights: Beginning with *View* and ending with *Full Control*, each access level builds upon the rights granted by the previous level.

However, you can also create and customize your own access levels; this can greatly reduce administrative and maintenance costs associated with security. Consider a situation in which an administrator must manage

two groups, sales managers and sales employees. Both groups need to access five reports in the BI platform system, but sales managers require more rights than sales employees. The predefined access levels do not meet the needs of either group. Instead of adding groups to each report as principals and modifying their rights in five different places, the administrator can create two new access levels, Sales Managers and Sales Employees. The administrator then adds both groups as principals to the reports and assigns the groups their respective access levels. When rights need to be modified, the administrator can modify the access levels. Because the access levels apply to both groups across all five reports, the rights those groups have to the reports are quickly updated.

Related Information

Working with access levels [page 129]

7.1.2 Advanced rights settings

To provide you with full control over object security, the CMC allows you to set advanced rights. These advanced rights provide increased flexibility as you define security for objects at a granular level.

Use advanced rights settings, for instance, if you need to customize a principal's rights to a particular object or set of objects. Most importantly, use advanced rights to explicitly deny a user or group any right that should not be permitted to change when, in the future, you make changes to group memberships or folder security levels.

The following table summarizes the options that you have when you set advanced rights.

Rights options

Icon	Rights option	Description
	Granted	The right is granted to a principal.
	Denied	The right is denied to a principal.
	Not Specified	The right is unspecified for a principal. By default, rights set to *Not Specified* are denied.
	Apply to Object	The right applies to the object. This option becomes available when you click *Granted* or *Denied*.
	Apply to Sub Object	The right applies to sub-objects. This option becomes available when you click *Granted* or *Denied*.

Related Information

Type-specific rights [page 121]

7.1.3 Inheritance

Rights are set on an object for a principal in order to control access to the object; however, it is impractical to set the explicit value of every possible right for every principal on every object. Consider a system with 100 rights, 1000 users, and 10,000 objects: to set rights explicitly on each object would require the CMS store billions of rights in its memory, and, importantly, require that an administrator manually set each one.

Inheritance patterns resolve this impracticality. With inheritance, the rights that users have to objects in the system come from a combination of their memberships in different groups and subgroups and from objects which have inherited rights from parent folders and subfolders. These users can inherit rights as the result of group membership; subgroups can inherit rights from parent groups; and both users and groups can inherit rights from parent folders.

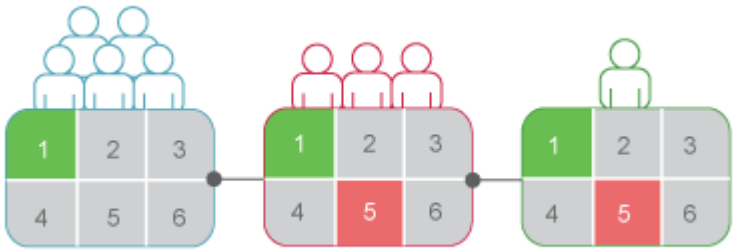
By default, users or groups who have rights to a folder will inherit the same rights for any object that are subsequently published to that folder. Consequently, the best strategy is to set the appropriate rights for users and groups at the folder level first, then publish objects to that folder.

The BI platform recognizes two types of inheritance: group inheritance and folder inheritance.

7.1.3.1 Group inheritance

Group inheritance allows principals to inherit rights as the result of group membership. Group inheritance proves especially useful when you organize all of your users into groups that coincide with your organization's current security conventions.

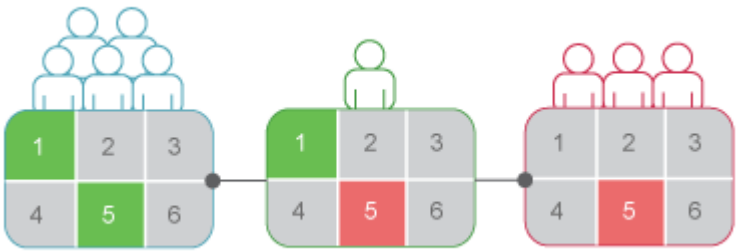
In “Group inheritance example 1”, you can see how group inheritance works. Red Group is a subgroup of Blue Group, so it inherits Blue Group's rights. In this case, it inherits right 1 as granted, and the rest of the rights as unspecified. Every member of Red Group inherits these rights. In addition, any other rights that are set on the subgroup are inherited by its members. In this example, Green User is a member of Red Group, and thus inherits right 1 as granted, rights 2, 3, 4, and 6 as not specified, and Right 5 as denied.



Group inheritance example 1

When group inheritance is enabled for a user who belongs to more than one group, the rights of all parent groups are considered when the system checks credentials. The user is denied any right that is explicitly denied in any parent group, and the user is denied any right that remains completely not specified; thus, the user is granted only those rights that are granted in one or more groups (explicitly or through access levels) and never explicitly denied.

In “Group inheritance example 2”, Green User is a member of two unrelated groups. From Blue Group, he inherits rights 1 and 5 as "granted" and the rest as not specified; however, because Green User also belongs to Red Group, and Red Group has been explicitly denied right 5, Green User's inheritance to right 5 from Blue Group is overridden.



Group inheritance example 2

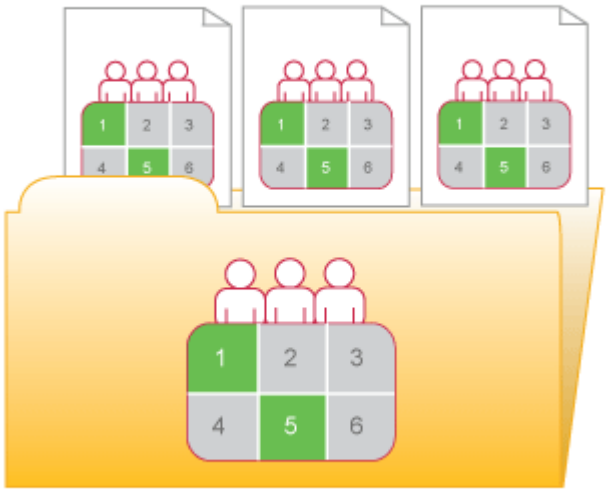
Related Information

Rights override [page 119]

7.1.3.2 Folder inheritance

Folder inheritance allows principals to inherit any rights that they have been granted on an object's parent folder. Folder inheritance proves especially useful when you organize BI platform content into a folder hierarchy that reflects your organization's current security conventions. For example, suppose that you create a folder called Sales Reports, and you provide your Sales group with *View On Demand* access to this folder. By default, every user that has rights to the Sales Reports folder will inherit the same rights to the reports that you subsequently publish to this folder. Consequently, the Sales group will have *View On Demand* access to all of the reports, and you need set the object rights only once, at the folder level.

In “Folder inheritance example”, rights have been set for Red Group on a folder. Rights 1 and 5 have been granted, while the rest have been left unspecified. With folder inheritance enabled, members of Red Group have rights on the object level identical to the rights of the group on the folder level. Rights 1 and 5 are inherited as granted, while the rest have been left unspecified.



Folder inheritance example

Related Information

Rights override [page 119]

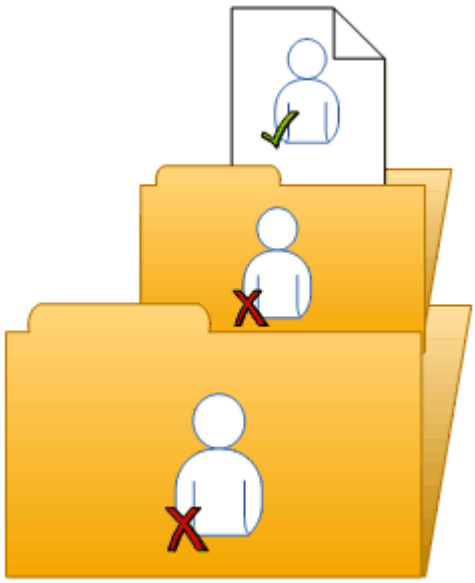
7.1.3.3 Rights override

Rights override is a rights behavior in which rights that are set on child objects override the rights set on parent objects. Rights override occurs under the following circumstances:

- In general, the rights that are set on child objects override the corresponding rights that are set on parent objects.
- In general, the rights that are set on subgroups or members of groups override the corresponding rights that are set on groups.

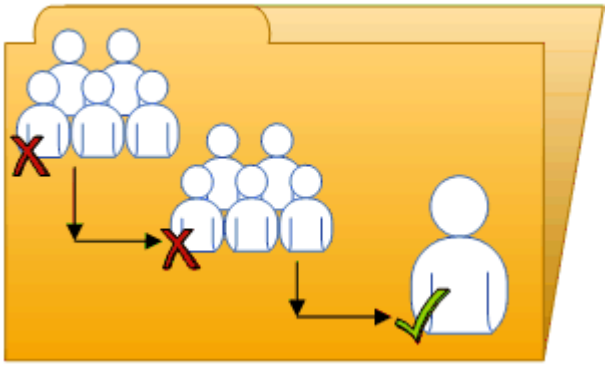
You do not need to disable inheritance to set customized rights on an object. The child object inherits the rights settings of the parent object except for the rights that are explicitly set on the child object. Also, any changes to rights settings on the parent object apply to the child object.

"Rights override example 1" illustrates how rights override works on parent and child objects. Blue User is denied the right to edit a folder's contents; the rights setting is inherited by the subfolder. However, an administrator grants Blue User *Edit* rights to a document in the subfolder. The *Edit* right that Blue User receives on the document overrides the inherited rights that come from the folder and subfolder.



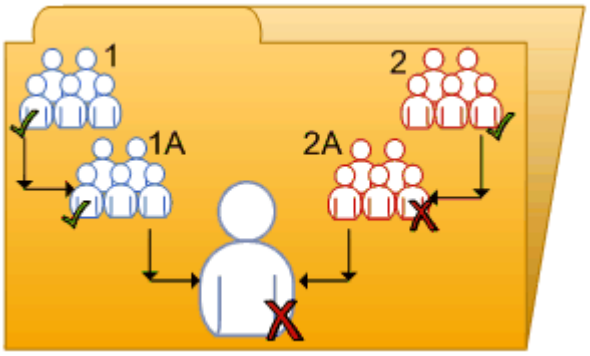
Rights override example 1

"Rights override example 2" illustrates how rights override works on members and groups. Blue Group is denied the right to edit a folder; Blue Subgroup inherits this rights setting. However, an administrator grants Blue User, who is a member of Blue Group and Blue Subgroup, *Edit* rights on the folder. The *Edit* rights that Blue User receives on the folder override the inherited rights that come from Blue Group and Blue Subgroup.



Rights override example 2

"Complex rights override" illustrates a situation where the effects of rights override are less obvious. Purple User is a member of subgroups 1A and 2A, which are in Groups 1 and 2, respectively. Groups 1 and 2 both have *Edit* rights on the folder. 1A inherits the *Edit* rights that Group 1 has, but an administrator denies *Edit* rights to 2A. The rights settings on 2A override the rights settings on Group 2 because of rights override. Therefore, Purple User inherits contradictory rights settings from 1A and 2A. 1A and 2A do not have a parent-child relationship, so rights override does not occur; that is, one sub-group's rights settings do not override another's because they have equal status. In the end, Purple User is denied *Edit* rights because of the "denial-based" rights model in the BI platform.



Complex rights override

Rights override lets you make minor adjustments to the rights settings on a child object without discarding all inherited rights settings. Consider a situation in which a sales manager needs to view confidential reports in the Confidential folder. The sales manager is part of the Sales group, which is denied access to the folder and its contents. The administrator grants the manager *View* rights on the Confidential folder and continues to deny the Sales group access. In this case, the *View* rights granted to the sales manager override the denied access that the manager inherits from membership in the Sales group.

7.1.3.4 Scope of rights

Scope of rights refers to the ability to control the extent of rights inheritance. To define the scope of a right, you decide whether the right applies to the object, its sub-objects, or both. By default, the scope of a right extends to both objects and sub-objects.

Scope of rights can be used to protect personal content in shared locations. Consider a situation in which the finance department has a shared Expense Claims folder that contains Personal Expense Claims subfolders for each employee. The employees want to be able to view the Expense Claims folder and add objects to it, but they also want to protect the contents of their Personal Expense Claims subfolders. The administrator grants all employees *View* and *Add* rights on the Expense Claims folder, and limits the scope of these rights to the Expense Claims folder only. This means that the *View* and *Add* rights do not apply to sub-objects in the Expense Claims folder. The administrator then grants employees *View* and *Add* rights on their own Personal Expense Claims subfolders.

Scope of rights can also limit the effective rights that a delegated administrator has. For example, a delegated administrator may have *Securely Modify Rights* and *Edit* rights on a folder, but the scope of these rights is limited to the folder only and does not apply to its sub-objects. The delegated administrator cannot grant these rights to another user on one of the folder's sub-objects.

7.1.4 Type-specific rights

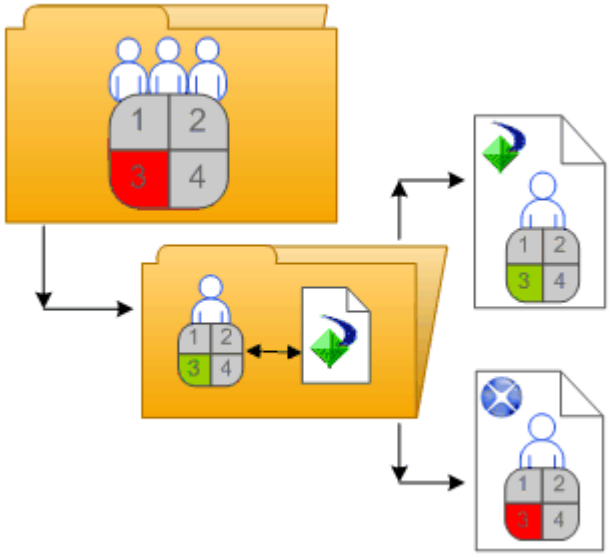
Type-specific rights are rights that affect specific object types only, such as Crystal reports, folders, or access levels. Type-specific rights consist of the following:

- General rights for the object type

These rights are identical to general global rights (for example, the right to add, delete, or edit an object), but you set them on specific object types to override the general global rights settings.

- Specific rights for the object type
  These rights are available for specific object types only. For example, the right to export a report's data appears for Crystal reports but not for Word documents.

The diagram "Type-specific rights example" illustrates how type-specific rights work. Here right 3 represents the right to edit an object. Blue Group is denied *Edit* rights on the top-level folder and granted *Edit* rights for Crystal reports in the folder and subfolder. These *Edit* rights are specific to Crystal reports and override the rights settings on a general global level. As a result, members of Blue Group have *Edit* rights for Crystal reports but not the XLF file in the subfolder.



Type-specific rights example

Type-specific rights are useful because they let you limit the rights of principals based on object type. Consider a situation in which an administrator wants employees to be able to add objects to a folder but not create subfolders. The administrator grants *Add* rights at the general global level for the folder, and then denies *Add* rights for the folder object type.

Rights are divided into the following collections based on the object types they apply to:

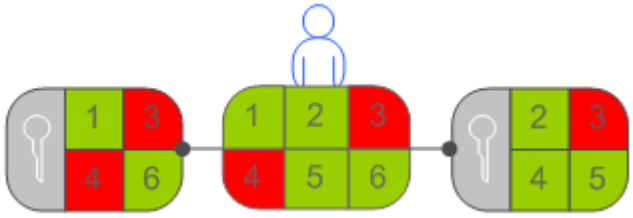
- *General*
  These rights affect all objects.
- *Content*
  These rights are divided according to particular content object types. Examples of content object types include Crystal reports, and Adobe Acrobat PDFs.
- *Application*
  These rights are divided according to which BI platform application they affect. Examples of applications include the CMC and BI launch pad.
- *System*
  These rights are divided according to which core system component they affect. Examples of core system components include Calendars, Events, and Users and Groups.

Type-specific rights are in the *Content*, *Application*, and *System* collections. In each collection, they are further divided into categories based on object type.

7.1.5 Determining effective rights

Keep these considerations in mind when you set rights on an object:

- Each access level grants some rights, denies some rights, and leaves the other rights unspecified. When a user is granted several access levels, the system aggregates the effective rights and denies any unspecified rights by default.
- When you assign multiple access levels to a principal on an object, the principal has the combination of each access level's rights. The user in "Multiple access levels" is assigned two access levels. One access level grants the user rights 3 and 4, while the other access level grants right 3 only. The effective rights for the user are 3 and 4.



Multiple access levels

- Advanced rights can be combined with access levels to customize the rights settings for a principal on an object. For example, if an advanced right and an access level are both assigned explicitly to a principal on an object, and the advanced right contradicts a right in the access level, the advanced right will override the right in the access level.
  Advanced rights can override their identical counterparts in access levels only when they are set on the same object for the same principal. For example, an advanced Add right set at the general global level can override the general Add right setting in an access level; it cannot override a type-specific Add right setting in an access level.
  However, advanced rights do not always override access levels. For example, a principal is denied an *Edit* right on a parent object. On the child object, the principal is assigned an access level that grants him the *Edit* right. In the end, the principal has *Edit* rights on the child object because the rights set on the child object override rights that are set on the parent object.
- Rights override makes it possible for rights set on a child object to override rights that are inherited from the parent object.

7.2 Managing security settings for objects in the CMC

You can manage security settings for most objects in the CMC with the security options on the *Manage* menu. These options let you assign principals to the access control list for an object, view the rights that a principal has, and modify the rights that the principal has to an object.

The specific details of security management vary according to your security needs and the type of object you are setting rights for. However, in general, the workflows for the following tasks are very similar:

- Viewing rights for a principal on an object.
- Assigning principals to an access control list for an object, and specifying which rights and access levels those principals have.
- Setting rights on a top-level folder in the BI platform.

7.2.1 To view rights for a principal on an object

Context

In general, you follow this workflow to view rights for a principal on an object.

Procedure

1. Select the object for which you want to view security settings.
2. Click *Manage* > *User Security*.
   The *User Security* dialog box appears and displays the access control list for the object.
3. Select a principal from the access control list, and click *View Security*

   The *Permissions Explorer* launches and displays a list of effective rights for the principal on the object. In addition, the *Permissions Explorer* lets you do the following:

   - Browse for another principal whose rights you want to view.
   - Filter the rights displayed according to these criteria:

     Assigned rights
     Granted rights
     Unassigned rights
     From access level
     Object type
     The name of the right
   - Sort the list of rights displayed in ascending or descending order according to these criteria:

     Collection
     Type
     Right name
     Right status (granted, denied, or unspecified)

   Additionally, you can click one of the links in the *Source* column to display the source of inherited rights.

7.2.2 To assign principals to an access control list for an object

Context

An access control list specifies the users that are granted or denied rights on an object. In general, you follow this workflow to assign a principal to an access control list, and to specify the rights that the principal has to the object.

Procedure

1. Select the object to which you want to add a principal.
2. Click *Manage* > *User Security*.
   The *User Security* dialog box appears and displays the access control list.
3. Click *Add Principals*.
   The *Add Principals* dialog box appears.
4. Move the users and groups you want to add as principals from the *Available users/groups* list to the *Selected users/groups* list.
5. Click *Add and Assign Security*.
6. Select the access levels you want to grant the principal.
7. Choose whether to enable or disable folder or group inheritance.

Next Steps

If necessary, you can also modify rights at a granular level to override certain rights in an access level.

Related Information

To modify security for a principal on an object [page 125]

7.2.3 To modify security for a principal on an object

Context

In general, it is recommended that you use access levels to assign rights to a principal. However, you may need to override certain granular rights in an access level sometimes. Advanced rights let you customize the rights

for a principal on top of the access levels the principal already has. In general, you follow this workflow to assign advanced rights to a principal on an object.

Procedure

1. Assign the principal to the access control list for the object.
2. When the principal has been added, go to *Manage* > *User Security* to display the access control list for the object.
3. Select the principal from the access control list, and click *Assign Security*.
   The *Assign Security* dialog box appears.
4. Click the *Advanced* tab.
5. Click *Add/Remove rights*.
6. Modify the rights for the principal.
   All the available rights are summarized in the *Rights Appendix*.

Related Information

To assign principals to an access control list for an object [page 125]

7.2.4 To set rights on a top-level folder in the BI platform

Context

In general, you follow this workflow to set rights on a top-level folder in the BI platform.

> **Note**
>
> For this release, principals require *View* rights on a container folder to be able to navigate in that folder and view its sub-objects. This means that principals require *View* rights on the top-level folder to view objects that are in folders. If you want to limit *View* rights for a principal, you can grant a principal *View* rights on a specific folder and set the scope of rights to apply to that folder only.

Procedure

1. Go to the CMC area that has the top-level folder you want to set rights for.
2. Click *Manage* > *Top-Level Security* > *All* `<Objects>`.
   Here `<Objects>` represents the contents of the top-level folder. If you are prompted for confirmation, click *OK*.

The *User Security* dialog box appears and displays the access control list for the top-level folder.

3. Assign the principal to the access control list for the top-level folder.
4. If necessary, assign advanced rights to the principal.

Related Information

To assign principals to an access control list for an object [page 125]
To modify security for a principal on an object [page 125]

7.2.5 Checking security settings for a principal

In some cases, you may want to know the objects to which a principal has been granted or denied access. You can use a security query to do this. Security queries let you determine which objects a principal has certain rights to and manage user rights. For each security query, you provide the following information:

- Query principal
  You specify the user or group that you want to run the security query for. You can specify one principal for each security query.
- Query permission
  You specify the right or rights you want to run the security query for, the status of these rights, and the object type these rights are set on. For example, you can run a security query for all reports that a principal can refresh, or for all reports that a principal cannot export.
- Query context
  You specify the CMC areas that you want the security query to search. For each area, you can choose whether to include sub-objects in the security query. A security query can have a maximum of four areas.

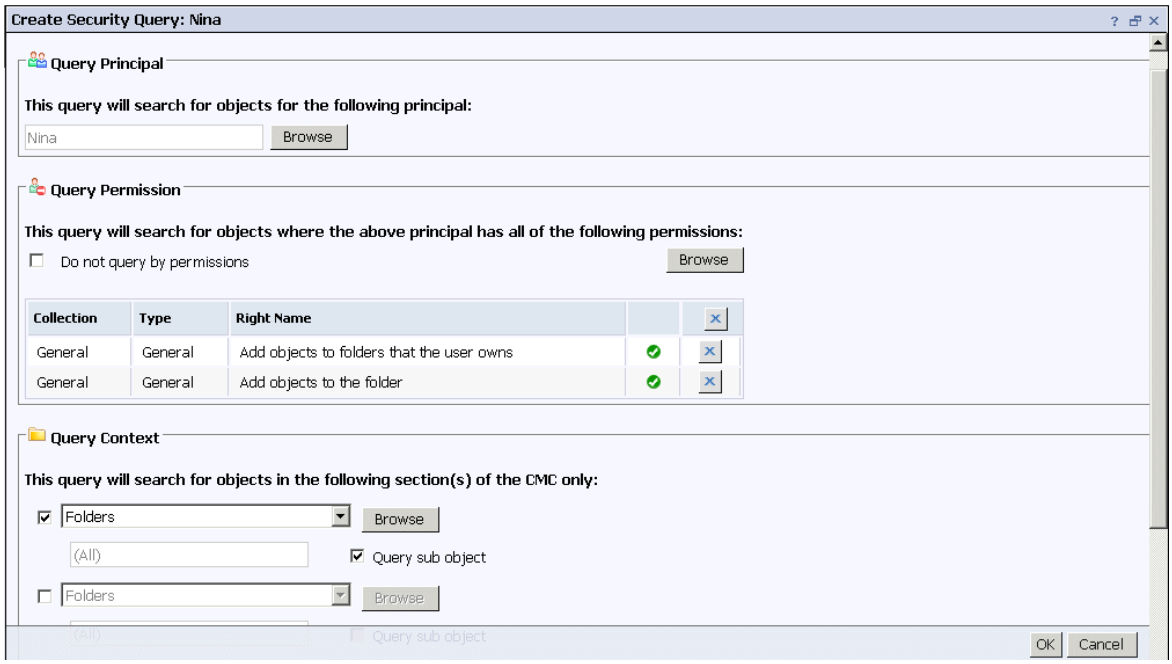
When you run a security query, the results appear in the *Query Results* area in the *Tree* panel under *Security Queries*. If you want to refine a security query, you can run a second query within the results from the first query.

Security queries are useful because they allow you to see the objects that a principal has certain rights to, and they provide the locations of these objects if you want to modify those rights. Consider a situation in which a sales employee is promoted to sales manager. The sales manager needs *Schedule* rights for Crystal reports that he only had *View* rights to previously, and these reports are in different folders. In this case, the administrator runs a security query for the sales manager's right to view Crystal reports in all folders and includes sub-objects in the query. After the security query runs, the administrator can see all Crystal reports that the sales manager has *View* rights for in the *Query Results* area. Because the *Details* panel displays the location of each Crystal report, the administrator can browse for each report and modify the sales manager's rights on it.

7.2.5.1 To run a security query

Procedure

1. In the *Users and Groups* area, in the *Details* panel, select the user or group that you want to run a security query for.
2. Click *Manage* > *Tools* > *Create Security Query*.



   The *Create Security Query* dialog box appears.
3. Ensure that the principal in the *Query Principal* area is correct.

   If you decide to run a security query for a different principal, you can click *Browse* to select another principal. In the *Browse for Query Principal* dialog box, expand *User List* or *Groups List* to browse for the principal, or search for the principal by name. When you are finished, click *OK* to return to the *Create Security Query* dialog box.
4. In the *Query Permission* area, specify the rights and the status of each right for which you want to run the query..
   - If you want to run a query for specific rights that the principal has on objects, click *Browse*, set the status of each right that you want to run the security query for, and click *OK*.

     > → Tip
     >
     > You can delete specific rights from the query by clicking the delete button next to the right, or delete all rights from the query by clicking the delete button in the header row.

   - If you want to run a general security query, select the *Do not query by permissions* check box. When you do this, the BI platform runs a general security query for all objects that have the principal in their access control lists regardless of the permissions that the principal has on the objects.
5. In the *Query Context* area, specify the CMC areas that you want to query.

a. Select a check box next to a list.
b. On the list, select a CMC area that you want to query.

   If you want to query a more specific location within an area (for example, a particular folder under Folders), click *Browse* to open the *Browse for Query Context* dialog box. In the *details* pane, select the folder you want to query, and click *OK*. When you return to the *Security Query* dialog box, the folder you specified appears in the box under the list.
c. Select *Query sub object*.
d. Repeat the steps above for each CMC area that you want to query.

> **Note**
>
> You can query a maximum of four areas.

6. Click *OK*.
   The security query runs and you are taken to the *Query Results* area.
7. To view the query results, in the *Tree* panel, expand *Security Queries* and click a query result.

> **→ Tip**
>
> Query results are listed according to the names of principals.

   The query results are displayed in the *Details* panel.

Next Steps

The *Query Results* area retains all security query results from a single user session until the user logs off. If you want to run the query again but with new specifications, click *Actions* > *Edit Query*. You can also rerun the exact same query by selecting the query and clicking *Actions* > *Rerun Query*. If you want to keep your security query results, click *Actions* > *Export* to export your security query results as a CSV file.

7.3 Working with access levels

You can do the following with access levels:

- Copy an existing access level, make changes to the copy, rename it, and save it as a new access level.
- Create, rename, and delete access levels.
- Modify the rights in an access level.
- Trace the relationship between access levels and other objects in the system.
- Replicate and manage access levels across sites.
- Use one of the predefined access levels in BI platform to set rights quickly and uniformly for many principals.

The following table summarizes the rights that each predefined access level contains.

Predefined access levels

Access level	Description	Rights involved
View	If set on the folder level, a principal can view the folder, objects within the folder, and each object's generated instances. If set at the object level, a principal can view the object, its history, and its generated instances.	• View objects • View document instances
Schedule	A principal can generate instances by scheduling an object to run against a specified data source once or on a recurring basis. The principal can view, delete, and pause the scheduling of instances that they own. They can also schedule to different formats and destinations, set parameters and database logon information, choose servers to process jobs, add contents to the folder, and copy the object or folder.	*View* access level rights, plus: • Schedule the document to run • Define server groups to process jobs • Copy objects to another folder • Schedule to destinations • Print the report's data • Export the report's data • Edit objects that the user owns • Delete instances that the user owns • Pause and resume document instances that the user owns
View On Demand	A principal can refresh data on demand against a data source.	*Schedule* access level rights, plus: • Refresh the report's data
Full Control	A principal has full administrative control of the object.	All available rights, including: • Add objects to the folder • Edit objects • Modify rights users have to objects • Delete objects • Delete instances

The following table summarizes the rights required to perform certain tasks on access levels.

Access level task	Rights required
Create an access level	*Add* right on the *Access Levels* top-level folder
View granular rights in an access level	*View* right on the access level
Assign an access level to a principal on an object	*View* right on the access level *Use the Access Level for Security Assignment* right on the access level *Modify Rights* right on the object, or *Securely Modify Rights* right on the object and the principal

Access level task	Rights required
	Note Users who have the *Securely Modify Rights* right and want to assign an access level to a principal must have that same access level assigned to themselves.
Modify an access level	*View* and *Edit* rights on the access level
Delete an access level	*View* and *Delete* rights on the access level
Clone an access level	*View* right on the access level *Copy* right on the access level *Add* right on the *Access Levels* top-level folder

7.3.1 Choosing between *View* and *View On Demand* access levels

When reporting over the web, the choice to use live or saved data is one of the most important decisions you'll make. Whichever choice you make, however, the BI platform displays the first page as quickly as possible, so you can see your report while the rest of the data is being processed. This section explains the difference between two predefined access levels that you can use to make this choice.

View On Demand access level

On-demand reporting gives users real-time access to live data, straight from the database server. Use live data to keep users up-to-date on constantly changing data, so they can access information that's accurate to the second. For instance, if the managers of a large distribution center need to keep track of inventory shipped on a continual basis, then live reporting is the way to give them the information they need.

Before providing live data for all your reports, however, consider whether or not you want all of your users hitting the database server on a continual basis. If the data isn't rapidly or constantly changing, then all those requests to the database do little more than increase network traffic and consume server resources. In such cases, you may prefer to schedule reports on a recurrent basis so that users can always view recent data (report instances) without hitting the database server.

Users require *View On Demand* access to refresh reports against the database.

View access level

To reduce the amount of network traffic and the number of hits on your database servers, you can schedule reports to be run at specified times. When the report has been run, users can view that report instance as needed, without triggering additional hits on the database.

Report instances are useful for dealing with data that isn't continually updated. When users navigate through report instances, and drill down for details on columns or charts, they don't access the database server directly; instead, they access the saved data. Consequently, reports with saved data not only minimize data transfer over the network, but also lighten the database server's workload.

For example, if your sales database is updated once a day, you can run the report on a similar schedule. Sales representatives then always have access to current sales data, but they are not hitting the database every time they open a report.

Users require only *View* access to display report instances.

7.3.2 To copy an existing access level

Context

This is the best way to create an access level if you want an access level that differs slightly from one of the existing access levels.

Procedure

1. Go to the *Access Levels* area.
2. In the *Details* panel, select an access level.

   > → Tip
   >
   > Select an access level that contains rights that are similar to what you want for your access level.

3. Click *Organize* > *Copy*.
   A copy of the access level you selected appears in the *Details* panel.

7.3.3 To create a new access level

Context

This is the best way to create an access level if you want an access level that differs greatly from one of the existing access levels.

Procedure

1. Go to the *Access Levels* area.

2. Click *Manage* > *New* > *Create Access Level*.
   The *Create New Access Level* dialog box appears.
3. Enter a title and description for your new access level, and then click *OK*.
   You return to the *Access Levels* area, and the new access level appears in the *Details* panel.

7.3.4 To rename an access level

Procedure

1. In the *Access Levels* area, in the *Details* panel, select the access level that you want to rename.
2. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
3. In the *Title* field, enter a new name for your access level, and then click *Save & Close*.
   You return to the *Access Levels* area.

7.3.5 To delete an access level

Procedure

1. In the *Access Levels* area, in the *Details* panel, select the access level that you want to delete.
2. Click *Manage* > *Delete Access Level*.

   > **Note**
   >
   > You cannot delete predefined access levels.

   A dialog box appears with information about the objects that this access level affects. If you do not want to delete the access level, click *Cancel* to exit the dialog box.
3. Click *Delete*.
   The access level is deleted, and you return to the *Access Levels* area.

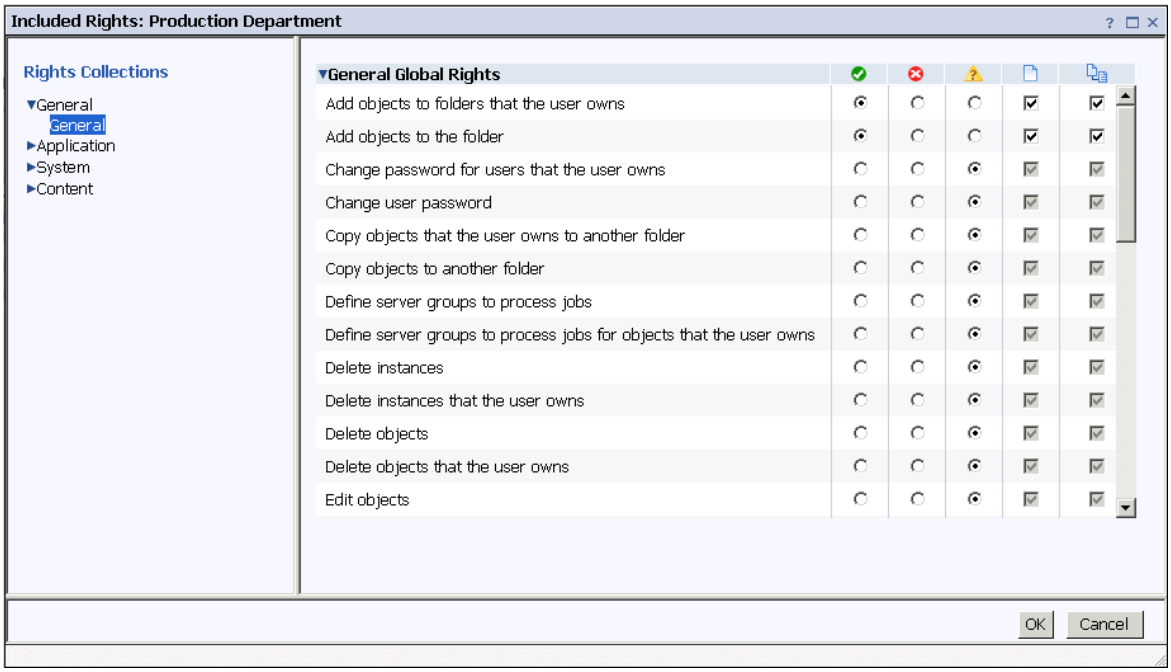
7.3.6 To modify rights in an access level

Context

To set rights for an access level, you first set general global rights that apply to all objects regardless of type, and then you specify when you want to override the general settings based on the specific object type.

Procedure

1. In the *Access Levels* area, in the *Details* panel, select the access level that you want to modify the rights for.
2. Click *Actions* > *Included Rights*.
   The *Included Rights* dialog box appears and displays a list of effective rights.
3. Click *Add/Remove Rights*.



   The *Included Rights* dialog box displays the rights collections for the access level in the navigation list. The *General Global Rights* section is expanded by default.
4. Set your general global rights.

   Each right can have a status of *Granted*, *Denied*, or *Not Specified*. You can also choose whether to apply that right to the object only, to apply it to sub-objects only, or both.
5. To set type-specific rights for the access level, in the navigation list, click the rights collection, and then click the sub-collection that applies to the object type you want to set the rights for.
6. When you have finished, click *OK*.
   You return to the list of effective rights.

7.3.7 Tracing the relationship between access levels and objects

Before you modify or delete an access level, it is important to confirm that any changes you make to the access level will not impact objects in the CMC negatively. You can do this by running a relationship query on the access level.

Relationship queries are useful for rights management because they allow you to see objects impacted by an access level in one convenient location. Consider a situation in which a company restructures its organization and merges two departments, Department A and Department B, into Department C. The administrator decides

to delete the access levels for Department A and Department B because these departments no longer exist. The administrator runs relationship queries for both access levels before deleting them. In the *Query Results* area, the administrator can see the objects that will be affected if the administrator deletes the access levels. The *Details* panel also shows the administrator the location of the objects in the CMC if the rights on the objects must be modified before the access levels are deleted.

> **Note**
>
> To view the list of affected objects, you must have *View* rights on those objects.

> **Note**
>
> Relationship query results for an access level only yield objects on which the access level is explicitly assigned. If an object uses an access level because of inheritance settings, that object does not appear in the query results.

7.3.8 Managing access levels across sites

Access levels are one of the objects that you can replicate from an Origin site to Destination sites. You can choose to replicate access levels if they appear in a replication object's access control list. For example, if a principal is granted access level A on a Crystal report and the Crystal report is replicated across sites, access level A is also replicated.

> **Note**
>
> If an access level with the same name exists in the Destination site, the access level replication will fail. You or the Destination site administrator must rename one of the access levels before replication.

After you replicate an access level across sites, keep the administration considerations in this section in mind.

Modifying replicated access levels in the Origin site

If a replicated access level is modified in the Origin site, the access level in the Destination site will be updated the next time the replication is scheduled to run. In two-way replication scenarios, if you modify a replicated access level in the Destination site, the access level in the Origin site changes.

> **Note**
>
> Ensure that changes to an access level in one site do not affect objects in other sites negatively. Consult your site administrators and advise them to run relationship queries for the replicated access level before you make any changes.

Modifying replicated access levels in the Destination site

> **Note**
>
> This applies to one-way replication only.

Any changes to replicated access levels made in a Destination site are not reflected in the Origin site. For example, a Destination site administrator can grant the right to schedule Crystal reports in the replicated access level even though this right was denied in the Origin site. As a result, although the access level names and replicated object names remain the same, the effective rights that principals have on objects may differ from Destination site to Destination site.

If the replicated access level differs between the Origin and Destination sites, the difference in effective rights will be detected the next time a Replication Job is scheduled to run. You can force the Origin site access level to override the Destination site access level, or allow the Destination site access level to remain intact. However, if you do not force the Origin site access level to override the Destination site access level, any objects pending Replication that use that access level will fail to replicate.

To restrict users from modifying replicated access levels in the Destination site, you can add Destination site users to the access level as principals, and grant those users *View* rights only. This means that Destination site users can view the access level but are unable to modify its rights settings or assign it to other users.

Related Information

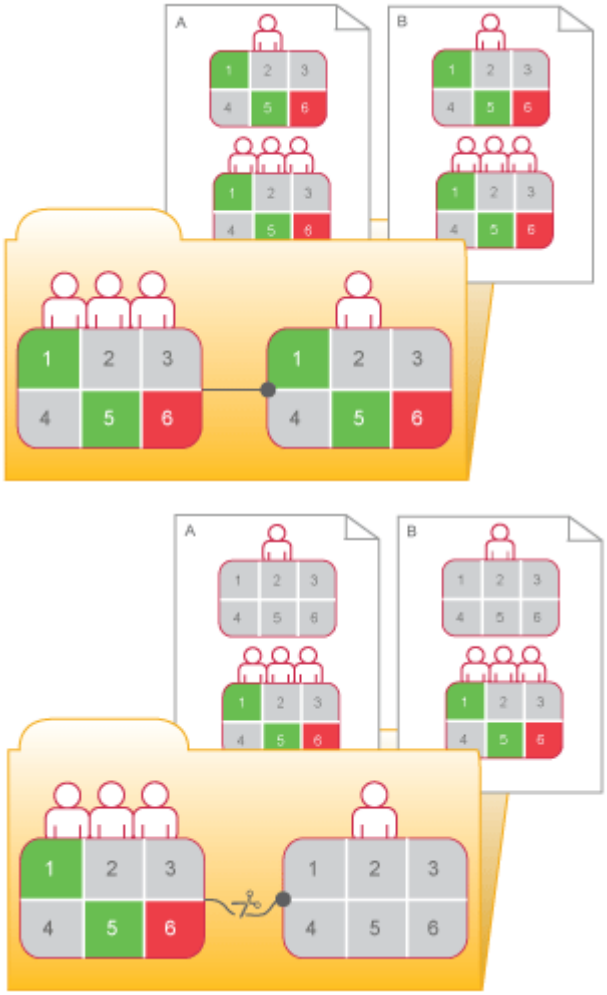
Federation [page 883]
Tracing the relationship between access levels and objects [page 134]

7.4 Breaking inheritance

Inheritance lets you manage your security settings without setting rights for each individual object. However, in some cases, you may not want rights to be inherited. For example, you may want to customize rights for each object. You can disable inheritance for a principal in an object's access control list. When you do this, you can choose whether to disable group inheritance, folder inheritance, or both.

> **Note**
>
> When inheritance is broken, it is broken for all rights; it is not possible to turn off inheritance for some rights but not for others.

In the diagram “Breaking inheritance”, group and folder inheritance are initially in effect. Red User inherits rights 1 and 5 as granted, rights 2, 3, and 4 as unspecified, and right 6 as explicitly denied. These rights, set on the folder level for the group, mean that Red User, and every other member of the group, has these rights on the folder's objects, A and B. When inheritance is broken on the folder level, Red User's set of rights to the objects in that folder is cleared until an administrator assigns new rights to him.



Breaking inheritance

7.4.1 To disable inheritance

Context

This procedure lets you disable group or folder inheritance, or both, for a principal on an object's access control list.

Procedure

1. Select the object that you want to disable inheritance for.
2. Click *Manage* > *User Security*.
   The *User Security* dialog box appears.
3. Select the principal that you want to disable inheritance for, and click *Assign Security*.
   The *Assign Security* dialog box appears.

4. Configure your inheritance settings.
    - If you want to disable group inheritance (the rights that the principal inherits from group membership), clear the *Inherit From Parent Group* check box.
    - If you want to disable folder inheritance (the rights settings that the object inherits from the folder), clear the *Inherit From Parent Folder* check box.
5. Click *OK*.

7.5 Using rights to delegate administration

Besides allowing you to control access to objects and settings, rights allow you to divide administrative tasks between functional groups within your organization. For example, you may want people from different departments to manage their own users and groups. Or you may have one administrator who handles high-level management of the BI platform, but you want all server management to be handled by people in your IT department.

Assuming that your group structure and folder structure align with your delegated-administration security structure, you should grant your delegated administrator rights to entire user groups, but grant the delegated administrator less than full rights on the users he controls. For example, you might not want the delegated administrator to edit user attributes or reassign them to different groups.

> **Note**
>
> Object migrations are best performed by members of the Administrators group, in particular the Administrator user account. To migrate an object, many related objects may also need to be migrated. Obtaining the required security rights for all the objects may not be possible for a delegated administrator account.

The "Rights for delegated administrators" table summarizes the rights required for delegated administrators to perform common actions.

Rights for delegated administrators

Action for delegated administrator	Rights required by the delegated administrator
Create new users	*Add* right on the top-level *Users* folder
Create new groups	*Add* right on the top-level *User Groups* folder
Delete any controlled groups, as well as individual users in those groups	*Delete* right on relevant groups
Delete only users that the delegated administrator creates	*Owner Delete* right on the top-level *Users* folder
Delete only users and groups that the delegated administrator creates	*Owner Delete* right on the top-level *User Groups* folder
Manipulate only users that the delegated creates (including adding those users to those groups)	*Owner Edit* and *Owner Securely Modify Rights* right on the top-level *Users* folder

Action for delegated administrator	Rights required by the delegated administrator
Manipulate only groups that the delegated administrator creates (including adding users to those groups)	*Owner Edit* and *Owner Securely Modify Rights* on the top-level *User Groups* folder
Modify passwords for users in their controlled groups	*Edit Password* right on relevant groups
Modify passwords only for principals the delegated administrator creates	*Owner Edit Password* right on top-level *Users* folder, or on relevant groups **Note** Setting the *Owner Edit Password* right on a group takes effect on a user only when you add the user to the relevant group.
Modify user names, description, other attributes, and reassign users to different groups	*Edit* right on relevant groups
Modify user names, description, other attributes, and reassign users to different groups, but only for users that the delegated administrator creates	*Owner Edit* right on top-level *Users* folder, or on relevant groups **Note** Setting the *Owner Edit* right on relevant groups takes effect on a user only when you add the user to the relevant group.

7.5.1 Choosing between "*Modify the rights users have to objects*" options

When you set up delegated administration, give your delegated administrator rights on the principals he will control. You may want to give her all rights (*Full Control*); however, it is good practice to use advanced rights settings to withhold the *Modify Rights* right and give your delegated administrator the *Securely Modify Rights* right instead. You may also give your administrator the *Securely Modify Rights Inheritance Settings* right instead of the *Modify Rights Inheritance Settings* right. The differences between these rights are summarized below.

Modify the rights users have to objects

This right allows a user to modify any right for any user on that object. For example, if user A has the rights *View objects* and *Modify the rights users have to object on an object*, user A can then change the rights for that object so he or any other user has full control of this object.

Securely modify the rights users have to objects

This right allows a user to grant, deny, or revert to unspecified only the rights he is already granted. For example, if user A has *View* and *Securely modify the rights users have to objects* rights, user A cannot give herself any more rights and can grant or deny to other users only these two rights (*View* and *Securely Modify Rights*). Additionally, user A can change only the rights for users on objects for which he has the *Securely Modify Rights* right.

These are all the conditions that must exist for user A to modify the rights for user B on object O:

- User A has the *Securely Modify Rights* right on object O.
- Each right or access level that user A is changing for user B is granted to A.
- User A has the *Securely Modify Rights* right on user B.
- If an access level is being assigned, User A has *Assign Access Level* right on the access level that is changing for user B.

Scope of rights can further limit the effective rights that a delegated administrator can assign. For example, a delegated administrator may have *Securely Modify Rights* and *Edit* rights on a folder, but the scope of these rights is limited to the folder only and does not apply to its sub-objects. Effectively, the delegated administrator can grant the *Edit* right on the folder (but not on its sub-objects) only, and with an "Apply to objects" scope only. On the other hand, if the delegated administrator is granted the *Edit* right on a folder with a scope of "Apply to sub-objects" only, she can grant other principals the *Edit* right with both scopes on the folder's sub-objects, but on the folder itself, she can only grant the *Edit* right with an "Apply to sub-objects" scope.

In addition, the delegated administrator will be restricted from modifying rights on those groups for other principals that she doesn't have the *Securely Modify Rights* right on. This is useful, for example, if you have two delegated administrators responsible for granting rights to different user groups for the same folder, but you don't want one delegated administrator to be able to deny access to the groups controlled by the other delegated administrator. The *Securely Modify Rights* right ensures this, since delegated administrators generally won't have the *Securely Modify Rights* right on each other.

Securely modify rights inheritance settings

This right allows a delegated administrator to modify inheritance settings for other principals on the objects that the delegated administrator has access to. To successfully modify the inheritance settings of other principals, a delegated administrator must have this right on the object and on the user accounts for the principals.

7.5.2 Owner rights

Owner rights are rights that apply only to the owner of the object on which rights are being checked. In the BI platform, the owner of an object is the principal who created the object; if that principal is ever deleted from the system, ownership reverts to the Administrator.

Owner rights are useful in managing owner-based security. For example, you may want to create an folder or hierarchy of folders in which various users can create and view documents, but can only modify or delete their

own documents. In addition, owner rights are useful for allowing users to manipulate instances of reports they create, but not others' instances. In the case of the scheduling access level, this permits users to edit, delete, pause and reschedule only their own instances.

Owner rights work similarly to their corresponding regular rights. However, owner rights are effective only when the principal has been granted owner rights but regular rights are denied or not specified.

7.6 Summary of recommendations for rights administration

Keep these considerations in mind for rights administration:

- Use access levels wherever possible. These predefined sets of rights simplify administration by grouping together rights associated with common user needs.
- Set rights and access levels on top-level folders. Enabling inheritance will allow these rights to be passed down through the system with minimal administrative intervention.
- Avoid breaking inheritance whenever possible. By doing so, you can reduce the amount of time it takes to secure the content that you have added to the BI platform.
- Set appropriate rights for users and groups at the folder level, then publish objects to that folder. By default, users or groups who have rights to a folder will inherit the same rights for any object that you subsequently publish to that folder.
- Organize users into user groups, assign access levels and rights to the entire group, and assign access levels and rights to specific members when necessary.
- Create individual administrator accounts for each administrator in the system and add them to the Administrators group to improve accountability for system changes.
- By default, the Everyone group is granted very limited rights to top-level folders in the BI platform. After installation, it is recommended that you review the rights of Everyone group members and assign security accordingly.

8 Securing the BI Platform

8.1 Security overview

This section details the ways in which the BI platform addresses enterprise security concerns, thereby providing administrators and system architects with answers to typical questions regarding security.

The BI platform architecture addresses the many security concerns that affect today's businesses and organizations. The current release supports features such as distributed security, single sign-on, resource access security, granular object rights, and third-party authentication in order to protect against unauthorized access.

Because the BI platform provides the framework for an increasing number of components from the Enterprise family of SAP BusinessObjects products, this section details the security features and related functionality to show how the framework itself enforces and maintains security. As such, this section does not provide explicit procedural details; instead, it focuses on conceptual information and provides links to key procedures.

After a brief introduction to security concepts for the system, details are provided for the following topics:

- How to use encryption and data processing security modes to protect data.
- How to set up the Secure Sockets Layer for BI platform deployments.
- Guidelines for setting up and maintaining firewalls for the BI platform.
- Configuring reverse proxy servers.

8.2 Secure use of program objects

If a user has schedule rights on program objects, then user has the right to run it.

For Java programs, users can do the following:

- Users can specify the main class. The author of the program must ensure that no secondary/test main class is left in the program unintentionally.
- Users can specify the class path. They shouldn't have the right to upload `jar` on the system. It could be used to execute specially crafted code.

General recommendations for securing program objects

- Don't give server login credential information to the user.
- Give minimal rights to the user account that runs the program on the server. Especially forbid access to the installation path of SAP BusinessObjects Business Intelligence Platform. For more information, see 3676830.

- It is recommended to select the option *Fail job* in *Applications* > *Central Management Console* > *Program Objects Rights*.
- It is recommended to use folders for access control. Program objects with different security levels should be put in different folders.

8.3 Disaster recovery planning

Certain steps must be taken to protect your organization's investment in the BI platform to ensure maximum continuity of function of lines of business in the event of a disaster. This section provides guidelines for drafting a disaster recovery plan for your organization. You can also check this SAP Note for more information.

General guidelines

- Perform regular system backups and send copies of some of the backup media offsite if necessary.
- Safely store all software media.
- Safely store all license documentation.

Specific guidelines

There are three system resources that require specific attention in terms of disaster recovery planning:

- Content in the file repository servers: this includes proprietary content such as reports. You should regularly back up this content - in the event of a disaster there is no way to regenerate such content without a regular backup process in place.
- The system database used by the CMS: this resource contains all the crucial metadata for your deployment such as user information, reports and other sensitive information that is particular to your organization.
- Database information key file (.dbinfo file): this resource contains the master key to the system database. If for some reason this key is not available, you will not be able to access the system database. It is highly recommended, after deploying the BI platform, that you store the password for this resource in a safe and known location. Without the password you will not be able to regenerate the file and therefore you will lose access to the system database.

8.4 General recommendations for securing your deployment

The following are recommended guidelines for securing your BI platform deployments.

- Use firewalls to protect the communication between the CMS and other system components. If possible, always hide your CMS behind the firewall. At the very least, ensure that the system database is safely behind the firewall.
- Add additional encryption to the File Repository Servers. Once the system is up and running, proprietary content will be stored in these servers. Add additional encryption through the OS or use a third-party tool.
- Deploy a reverse proxy server in front of the web application servers in order to hide them behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, therefore hiding private IP addresses.
- Strictly enforce corporate password policies. Ensure that user passwords are routinely changed.
- If you have opted to install the system database and web application server provided with the BI platform, you should access the relevant documentation to ensure these components are deployed with adequate security configurations.
- Use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your deployment.
- Ensure that the platform installation directory and subdirectories are secured. Sensitive temporary data may be stored in these directories during system operation.
- Access to the Central Management Console (CMC) should be restricted to local access only. For information on deployment options for the CMC see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
- By default, Web Intelligence error messages include database schema information. To show error messages without the database schema information, perform the following steps:
  1. Open the `WebIContainer_ServerDescriptor.xml` configuration file for editing. By default, it is located at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64config`.
  2. Change the value of this parameter to False: `WebiParamDetailedDbErrorsEnabled = False`.

> ⚠ Caution
>
> Placeholders other than intended for editing should not be changed in any means. System Administrator should ensure that only the right person from the Administrator group (who are intended for the Node management) should have the edit rights on the Node. All other users including other members of the administrator group should be restricted to view/manage the Node objects by applying the proper security rights. In case if any of the placeholder values is corrupted accidentally and CMS is not coming up, refer to the following SAP Note 3269127.

> ⓘ Note
>
> Please refer to the following SAP Knowledge Base Article 3278916 to know how to restrict placeholders being modified to avoid possible malicious interference with the BI landscape.

Related Information

Configuring the SSL protocol [page 180]
Password restrictions [page 151]
Configuring security for bundled third-party servers [page 145]

8.5 Configuring security for bundled third-party servers

If you have opted to install third-party server components that are bundled with the BI platform, we recommend checking the security sections of the official documentation for SAP SQL Anywhere and Apache Tomcat.

8.6 Authentication

8.6.1 Active trust relationship

In a networked environment, a trust relationship between two domains is generally a connection that allows one domain to recognize users who have been authenticated by the other domain. While maintaining security, the trust relationship allows users to access resources in multiple domains without repeatedly having to provide their credentials.

Within the BI platform environment, the active trust relationship works similarly to provide each user with seamless access to resources across the system. Once the user has been authenticated and granted an active session, all other BI platform components can process the user's requests and actions without prompting for credentials. As such, the active trust relationship provides the basis for the BI platform's distributed security.

8.6.1.1 Logon tokens

A logon token is an encoded string that defines its own usage attributes and contains a user's session information. The logon token's usage attributes are specified when the logon token is generated. These attributes allow restrictions to be placed upon the logon token to reduce the chance of the logon token being used by malicious users. The current logon token usage attributes are:

- *Number of minutes*
  This attribute restricts the lifetime of the logon token.
- *Number of logons*
  This attribute restricts the number of times that the logon token can be used to log on to the BI platform.

Both attributes hinder malicious users from gaining unauthorized access to the BI platform with logon tokens retrieved from legitimate users.

> **Note**
>
> Storing a logon token in a cookie is a potential security risk if the network between the browser and application or web server is insecure – for example if the connection is made over a public network and is not using SSL or Trusted Authentication. It is good practice to use Secure Sockets Layer (SSL) to reduce security risk between the browser and application or web server.

When the logon cookie has been disabled, and the web server or web browser times out, the user is presented with the logon screen. When the cookie is enabled, and the server or browser times out, the user is seamlessly

logged back onto the system. However, because state information is tied to the web session, the user's state is lost. For example, if the user had a navigation tree expanded and a particular item selected, the tree is reset.

For the BI platform, the default is to have logon tokens enabled in the web client, however, you can disable logon tokens for BI launch pad. When you disable the logon tokens in the client, the user session will be limited by the web server or web browser timeout. When that session expires, the user will be required to log in to the BI platform again.

8.6.1.2 Ticket mechanism for distributed security

Enterprise systems dedicated to serving a large number of users typically require some form of distributed security. An enterprise system may require distributed security to support features such the transfer of trust (the ability to allow another component to act on behalf of the user).

The BI platform addresses distributed security by implementing a ticket mechanism (one that is similar to the Kerberos ticket mechanism). The CMS grants tickets that authorize components to perform actions on behalf of a particular user. In the BI platform, the ticket is referred to as the logon token.

This logon token is most commonly used over the Web. When users are first authenticated by the BI platform they receive logon tokens from the CMS. The user's web browser caches this logon token. When the user makes a new request, other BI platform components can read the logon token from the user's web browser.

8.6.2 Trusted Authentication

Context

Trusted Authentication is no longer using a shared secret. Web Application servers must be configured in the application Authorized URL Configuration. It is no longer possible to configure Trusted Authentication without HTTPS due to security reasons.

The legacy implementation of Trusted Authentication was based on a global secret. If you have enabled Trusted Authentication in a previous version of Business Intelligence, it will still work. It is recommended to switch to the new configuration. Once it is working, the legacy feature can be disabled permanently with the following steps:

Procedure

1. In the Central Management Console, in Manage Authentication, click *Enterprise*.
2. In section Trusted Authentication, uncheck *Trusted Authentication is enabled* and click *Update*.
3. In Organize Servers, restart one Central Management Server, or if there is only one, restarts all the servers.

4. Enable Trusted Authentication again in the Central Management Console.
   For more information, see 3525794.

8.6.2.1 Securing the trusted URL

The trusted URL must be secured to prevent unauthorized access. You can apply one of the following protection mechanisms:

- **Network segregation**
  Separate the network into an external network for user access to the web applications and an internal network for communication between the web applications and the backend server. If the internal network is considered trusted, block access to the trusted URL from the external network.
- **Client certificate authentication**
  Configure client certificate authentication on the trusted URL to ensure that only authenticated clients can access it.

For more information, see Implementing client certificate authentication on the trusted URL [page 249].

8.7 Sessions and session tracking

In general, a session is a client-server connection that enables the exchange of information between the two computers. A session's state is a set of data that describes the session's attributes, its configuration, or its content. When you establish a client-server connection over the Web, the nature of HTTP limits the duration of each session to a single page of information; thus, your web browser retains the state of each session in memory only for as long as any single Web page is displayed. As soon as you move from one web page to another, the state of the first session is discarded and replaced with the state of the next session. Consequently, Web sites and Web applications must somehow store the state of one session if they need to reuse its information in another.

The BI platform uses two common methods to store session state:

- Cookies—A cookie is a small text file that stores session state on the client side: the user's web browser caches the cookie for later use. The BI platform logon token is an example of this method.
- Session variables—A session variable is a portion of memory that stores session state on the server side. When the BI platform grants a user an active identity on the system, information such as the user's authentication type is stored in a session variable. So long as the session is maintained, the system neither has to prompt the user for the information a second time nor has to repeat any task that is necessary for the completion of the next request.
  For Java deployments, the session is used to handle .jsp requests; for .NET deployments, the session is used to handle .aspx requests.

> **Note**
>
> Ideally, the system should preserve the session variable while the user is active on the system. And, to ensure security and to minimize resource usage, the system should destroy the session variable as soon as the user has finished working on the system. However, because the interaction between a web browser and

a web server can be stateless, it can be difficult to know when users leave the system, if they do not log off explicitly. To address this issue, the BI platform implements session tracking.

8.7.1 CMS session tracking

The CMS implements a simple tracking algorithm. When a user logs on, the user is granted a CMS session, which the CMS preserves until the user logs off, or until the web application server session variable is released.

The web application server session is designed to notify the CMS on a recurring basis that it is still active, so the CMS session is retained so long as the web application server session exists. If the web application server session fails to communicate with the CMS for a ten-minute time period, the CMS destroys the CMS session. This handles scenarios where client-side components shut down irregularly.

8.7.2 Managing sessions

You can view and terminate sessions in the CMC.

You can view and terminate user sessions in the Central Management Console (CMC). For example, you may want to see which users are using multiple sessions. Or, you may want to terminate sessions consuming too many system resources, or very old sessions. You might also need to terminate sessions when preparing for system downtime or upgrades.

8.7.2.1 To view the session list

View sessions in the CMC.

Context

You can view a list of sessions in the Central Management Console.

Procedure

1. Log in to the CMC as an administrator.
2. From the *Manage* area, click *Sessions*.

Results

The list of user sessions for the cluster is displayed. You can click the column headers to sort the list by user name, by the number of open sessions, or by logon times. You can also click the user name or session count or logon time to display details for that user's sessions in the lower pane.

8.7.2.2 To terminate sessions

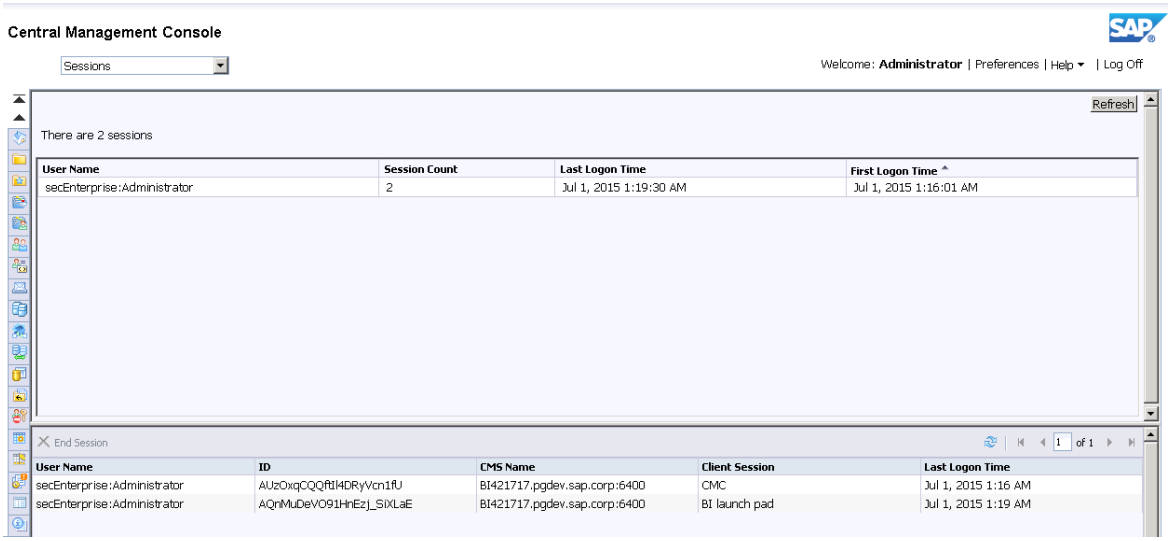
Terminate sessions in the CMC.

Context

You can terminate single or multiple sessions.

Procedure

1. Log in to the CMC as an administrator.
2. From the *Manage* area, click *Sessions*.
   The list of user sessions for the cluster is displayed.



3. Click a user name or session count or logon time, to display a user's sessions in the lower pane.
4. Click to select a single session, or `CTRL` + `click` to select multiple sessions.
5. Click *End Session*.

Results

> **Note**
>
> The User session is released once the user closes the browser.

> **Note**
>
> To terminate sessions, you must have the “Edit objects” right on the CMS object.

> **Note**
>
> You cannot terminate your current administrator session.

8.7.3 Script to clear Stale Sessions

Script

A script is introduced to clear the stale sessions and free the unused licenses to make them available for the users who are waiting to login. This script continues to execute until it is closed manually and it checks for the stale sessions and terminates them in every 10 mins interval.

- For Windows, you can find a script here: `<BI_Install_Dir>\SAP BusinessObjects Enterprise XI 4.0\java\lib\StaleSessionCleaner.jar`
- For Unix, you can find a script here: `<BI_Install_Dir>/sap_bobj/enterprise_xi40/java/lib/StaleSessionCleaner.jar`

The Syntax used for the script is

> **Code Syntax**
>
> ```
> java -jar StaleSessionCleaner.jar <username> <password>
> <machine:port><authentication> <logdir>
> ```

8.8 Environment protection

Environment protection refers to the security of the overall environment in which client and server components communicate. Although the Internet and web-based systems are increasingly popular due to their flexibility and range of functionality, they operate in an environment that can be difficult to secure. When you deploy the BI platform, environment protection is divided into two areas of communication: web browser to web server, and web server to BI platform.

8.8.1 Web browser to web server

When data is transmitted between the web browser and the web server, some degree of security is usually required. Relevant security measures usually involve two general tasks:

- Ensuring that the communication of data is secure.
- Ensuring that only valid users retrieve information from the web server.

> ⓘ Note
>
> These tasks are typically handled by web servers through various security mechanisms, including the Secure Sockets Layer (SSL) protocol, and other such mechanisms. It is good practice to use SSL to reduce security risk between the browser and application or web server.

You must secure communication between the web browser and the web server independently of the BI platform. For details on securing client connections, refer to your web server documentation.

8.8.2 Web server to BI platform

Firewalls are commonly used to secure the area of communication between the web server and the rest of the corporate intranet (including the BI platform). The platform supports firewalls that use IP filtering or static network address translation (NAT). Supported environments can involve multiple firewalls, web servers, or application servers.

8.8.3 Protection against malicious logon attempts

No matter how secure a system is, there is often at least one location that is vulnerable to attack: the location where users connect to the system. It is nearly impossible to protect this location completely, because the process of simply guessing a valid user name and password remains a viable way to attempt to "crack" the system.

The BI platform implements several techniques to reduce the probability of a malicious user achieving access to the system. The various restrictions listed below apply only to Enterprise accounts—that is, the restrictions do not apply to accounts that you have mapped to an external user database (LDAP or Windows AD). Generally, however, your external system will enable you to place similar restrictions on the external accounts.

8.8.4 Password restrictions

Password restrictions ensure that users authenticating the default Enterprise authentication create passwords that are relatively complex. You can enable the following options:

1. Enforce mixed-case passwords
   This option ensures that passwords contain at least one upper-case and one lower-case character in the password . This option is checked by default unless modified by the Administrator.

2. Enforce numeral(s) passwords
   This option ensures that passwords contain at least one numeric character.
3. Enforce special character passwords
   This option ensures that passwords contain at least one special character.

By enforcing a minimum complexity for passwords, you decrease a malicious user's chances of simply guessing a valid user's password.

8.8.5 Logon restrictions

Logon restrictions serve primarily to prevent dictionary attacks (a method whereby a malicious user obtains a valid user name and attempts to learn the corresponding password by trying every word in a dictionary). With the speed of modern hardware, malicious programs can guess millions of passwords per minute. To prevent dictionary attacks, the BI platform has an internal mechanism that enforces a time delay (0.5–1.0 second) between logon attempts. In addition, the platform provides several customizable options that you can use to reduce the risk of a dictionary attack:

- Disable accounts after N failed attempts to log on
- Reset failed logon count after N minute(s)
- Re-enable account after N minute(s)

8.8.6 User restrictions

User restrictions ensure that users authenticating the default Enterprise authentication create new passwords on a regular basis. You can enable the following options:

- Must change password every N day(s)
- Cannot reuse the N most recent password(s)
- Must wait N minute(s) to change password

These options are useful in a number of ways. Firstly, any malicious user attempting a dictionary attack will have to recommence every time passwords change. And, because password changes are based on each user's first logon time, the malicious user cannot easily determine when any particular password will change. Additionally, even if a malicious user does guess or otherwise obtain another user's credentials, they are valid only for a limited time.

8.8.7 Guest account restrictions

The BI platform supports anonymous single sign-on for the Guest account. Thus, when users connect to the BI platform without specifying a user name and password, the system logs them on automatically under the Guest account. If you assign a secure password to the Guest account, or if you disable the Guest account entirely, you disable this default behavior.

8.9 Auditing security configuration modifications

Any changes to default security configurations for the following will not be audited by the BI platform:

- Properties files for the web applications (BOE, web services)
- TrustedPrincipal.conf
- Customization performed on BI launch pad and Open Document

In general, any security configuration modifications performed outside the CMC will not be audited. This also applies to modifications performed though the Central Configuration Manager (CCM). Changes committed through the CMC can be audited.

8.10 Processing extensions

The BI platform allows you to further secure your reporting environment through the use of customized processing extensions. A processing extension is a dynamically loaded library of code that applies business logic to particular BI platform view or schedule requests before they are processed by the system.

Through its support for processing extensions, the BI platform administration SDK essentially exposes a "handle" that allows developers to intercept the request. Developers can then append selection formulas to the request before the report is processed.

A typical example is a report-processing extension that enforces row-level security. This type of security restricts data access by row within one or more database tables. The developer writes a dynamically loaded library that intercepts view or schedule requests for a report (before the requests are processed by a Job Server, Processing Server, or Report Application Server). The developer's code first determines the user who owns the processing job; then it looks up the user's data-access privileges in a third-party system. The code then generates and appends a record selection formula to the report in order to limit the data returned from the database. In this case, the processing extension serves as a way to incorporate customized row-level security into the BI platform environment.

By enabling processing extensions, you configure the appropriate BI platform server components to dynamically load your processing extensions at runtime. Included in the SDK is a fully documented API that developers can use to write processing extensions. For more information, see the developer documentation available on your product distribution.

8.11 Virus Scan Interface

You can commit different kinds of files (Adobe Acrobat, Microsoft Excel, Microsoft Word, Microsoft Powerpoint, Lumira, Crystal Reports, Web Intelligence, etc.) to the BI platform via the CMC, BI launch pad, Rest Web Services, and custom SDK applications. These files are subjected to size check (to ensure the file size is not zero) and permission check on destination directory. With the introduction of Virus Scan Interface in BI 4.2 SP4, files you commit to the BI platform are also committed to virus scan to ensure that the content of such files is not infected and is virus-free.

Files are subjected to virus scan when you:

- Add a new file
- 'Save as' a document
- Copy a document
- 'Send to BI Inbox' a document
- Create an instance of a document
- Or perform any operation that commits a new file into the file repository servers.

> **Note**
>
> Only files that are newly committed to the BI platform in BI 4.2 SP4 (after you enable virus scan) are subjected to a virus scan.

8.11.1 Enabling Virus Scan

You can enable virus scan for files committed to the BI platform for both the input and the output file repository servers.

Prerequisites

You have downloaded a Virus Scan Adapter (VSA) library. For more details, see KBA 1494278 - NW-VSI: Summary of Virus Scan Adapters for SAP Integration.

> **Note**
>
> If you need support for any new platform or vendor, contact the vendors regarding the same.

Context

To enable virus scan in the input file repository server, perform the following:

Procedure

1. Log on to the CMC.
2. Navigate to *Servers* > *Servers List*.
3. Right-click on the input file repository server, and select *Properties* from the dropdown.

   The *Properties* window appears.

4. In the *Input Filestore Service* section, select the *Enable Virus Scan* checkbox.
5. In the *Virus Scan Adapter File Location* field, enter the absolute path to the virus scan adapter library file.
6. Choose *Save & Close*.

> **Note**
>
> - By default, virus scan is disabled for all files committed to the BI platform in BI 4.2 SP4.
> - You can enable virus scan using either GUI or CLI. The command line argument you need to provide in the file repository servers for enabling virus scan is `vsaFileLoc`.
> - You can follow similar steps to enable virus scan in the Output File Repository Server. If you have multiple input and output file repository servers, ensure to enable virus scan on each of the servers.
> - You need to restart the file repository servers after you enable virus scan for the changes to take effect.

8.12 BI platform data security

Administrators of BI platform systems manage the way sensitive data is secured through the following:

- A security setting at the cluster level that determines which applications and clients can access the CMS. This setting is managed through the Central Configuration Manager.
- A two-key cryptography system that controls both access to the CMS repository, and keys used to encrypt/decrypt objects within the repository. Access to the CMS repository is set via the Central Configuration Manager, while the Central Management Console has a dedicated management area for cryptographic keys.

These features allow administrators to set BI platform deployments to particular data security compliance levels and to manage encryption keys used to encrypt and decrypt data within the CMS repository.

8.12.1 Data processing security modes

The BI platform can operate in two possible data processing security modes:

- The default data processing security mode. In certain instances, systems running in this mode will use hard-coded encryption keys and do not follow a specific standard. The default mode enables backward compatibility with previous versions of BI platform client tools and applications.
- A data security mode designed to meet guidelines stipulated by the Federal Information Processing Standard (FIPS) - specifically FIPS 140-2. In this mode FIPS-compliant algorithms and cryptographic modules are used to protect sensitive data. When the platform runs in FIPS-compliant mode, all clients tools and applications that do not meet FIPS guidelines are automatically disabled. The platform client tools and applications are designed to meet the FIPS 140-2 standard. Older clients and applications will not work when the BI platform is running in FIPS-compliant mode.

The data processing mode is transparent to system users. In both data processing security modes, sensitive data is encrypted and decrypted in the background by an internal encryption engine.

It is recommended that you use the FIPS-compliant mode in the following circumstances:

- Your BI platform deployment will not need to use or interact with any legacy BI platform client tools or applications.
- Your organization's data processing standards and guidelines prohibit the use of hard-coded encryption keys.
- Your organization is required to secure sensitive data according to FIPS 140-2 regulations.

The data processing security mode is set through the Central Configuration Manager on both Windows and UNIX platforms. Every node in a clustered environment must bet set to the same mode.

8.12.1.1 To turn on FIPS-compliant mode on Windows

Context

By default, FIPS-compliant mode is turned on when the BI platform is installed.

Procedure

1. To start the CCM, click *Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *Central Configuration Manager*.
2. In the CCM, right-click the Server Intelligence Agent (SIA) and select *Stop*.

   > ⚠ Caution
   >
   > Do not proceed to step 3 until the SIA status is Stopped.

3. Right-click the SIA and select *Properties*.
   The *Properties* dialog box appears, displaying the *Properties* tab.
4. Add `-fips` to the *Command* field, and click *Apply*.
5. Click *OK* to close the *Properties* dialog box.
6. Restart the SIA.

Results

The SIA is now operating in FIPS-complaint mode.

Next Steps

You must turn on the FIPS-compliant setting on all SIAs in your BI platform deployment.

8.12.1.2 To turn on FIPS-compliant mode on UNIX

Prerequisites

All nodes in your BI platform deployment must be stopped before attempting the following procedure.

Context

By default, FIPS-compliant mode is off after the BI platform is installed. Use the instructions below to turn on the FIPS-compliant setting for all nodes in your deployment.

Procedure

1. From the `<INSTALLDIR>/sap_bobj` directory, open the `ccm.config` file for editing.
2. Add `-fips` to the node launch command parameter.

   The node launch command parameter is displayed in this format: `<NODENAME>LAUNCH`. For example, for a node named "SAP", the node launch command parameter is `SAPLAUNCH`.
3. Save your changes and *Exit*.
4. Restart the node.

Results

The node is now operating in FIPS-complaint mode.

Next Steps

You must turn on the FIPS-compliant setting on all the nodes in your BI platform deployment.

8.12.1.3 To turn off FIPS-compliant mode on Windows

Prerequisites

All servers in your BI platform deployment must be stopped before attempting the following procedure.

Context

If your deployment is running on FIPS-compliant mode, use the following instructions to turn off the setting.

Procedure

1. In the CCM, right-click the Server Intelligence Agent (SIA) and choose *Stop*.

   > ⚠ Caution
   >
   > Do not proceed to Step 2 until the node status is marked as *Stopped*.

2. Right-click the SIA and choose *Properties*.
   The *Properties* dialog box appears with the *Properties* tab displayed.
3. Remove `-FIPS` from the *Command* field and click *Apply*.
4. Click *OK* to close the *Properties* dialog box.
5. Restart the SIA.

8.12.2 Administrator accounts

The BI platform automatically creates an initial Administrator account. We recommend creating an account in the Administrators group for each person.

The Administrator user is automatically granted the *Modify the rights users have to objects* right. Once you've created the administrator's account, remember to disable the initial Administrator account.

8.12.3 Connection rights

By default, administrators have access to connections details including passwords if the connections are defined with credentials.

This section explains how to apply the principle of least privilege on connections if administrators are not supposed to access data sources.

Restricting the "Download Connection Locally" right

The *Download Connection Locally* right is only strictly necessary for users managing the connections (see Connection rights [page 1053]). It should be granted only to individual users, not to groups. If a group has the right, any user added the group can have access to the connections details.

To fully secure the connections:

1. Grant the *Download Connection Locally* right to users managing the connections.
2. Deny the *Download Connection Locally* on the top folder of Connections for the Administrators and Universe Designers Users groups.

To prevent users from granting themselves the right, see the section below.

Securing the "Modify rights users have to objects right"

The default *Modify rights users have to objects* right allows users to grant a right even if they don't have it themselves. For connections, it must be replaced by the *Securely modify rights users have to objects* right. If Administrators don't have the *Download Connection Locally* right, they must not have the right to grant it to other users.

On top level Connections folder:

1. Grant the Administrators and Universe Designer groups the *Securely modify rights users have to objects* right.
2. Grant the right *Securely modify rights users have to objects* to users managing the connections as defined in the previous section. They'll have the right to grant the *Download Connection Locally* right.
3. Deny the Administrators and Universe Designer groups the *Modify rights users have to objects* right.

8.13 Cryptography in the BI platform

Sensitive Data

BI platform cryptography is designed to protect sensitive data stored in the CMS repository. Sensitive data includes user credentials, data source connectivity data, and any other info objects that store passwords. This data is encrypted to ensure privacy, keep it free from corruption, and maintain access control. All the requisite encryption resources (including the encryption engine, crypto libraries) are installed by default on each BI platform deployment.

The BI platform system uses a two-key cryptography system.

Cryptographic Keys

Encryption and decryption of sensitive data is handled in the background through the SDK interacting with the internal encryption engine. System administrators manage data security through symmetric encryption keys without directly encrypting or decrypting specific data blocks.

In the BI platform, symmetric encryption keys known as Cryptographic Keys are used to encrypt/decrypt sensitive data. The Central Management Console has a dedicated management area for cryptographic keys. Use the *Cryptographic Keys* to view, generate, deactivate, revoke, and delete keys. The system ensures that any key required to decrypt sensitive data cannot be deleted.

Cluster Keys

Cluster keys are symmetric key wrapping keys that protect cryptographic keys stored in the CMS repository. Using symmetric key algorithms, cluster keys maintain a level of access control to the CMS repository. Each node in the BI platform is assigned a cluster key during installation setup. System administrators can use the CCM to reset the cluster key.

8.13.1 Working with cluster keys

During the installation setup for the BI platform, an eight character cluster key is created for the Server Intelligence Agent. This key is used to encrypt all the cryptographic keys in the CMS repository. Without the correct cluster key, you cannot access the CMS.

The cluster key is stored in encrypted format in a `dbinfo` file. The `dbinfo` filename follows this convention: `_boe_<sia_name>.dbinfo`, where `<sia_name>` is the name of the Server Intelligence Agent for the cluster.

On Windows, the file is stored in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

On Unix systems, the file is stored in the platform directory under `<INSTALLDIR>/sap_bobj/enterprise_xi40/`:

Unix platform	Platform directory
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`

> **Note**
>
> The cluster key for any given node cannot be retrieved from the `dbinfo` file. It is recommended that system administrators take considered and careful measures to protect cluster keys.

Only users with administrative privileges can reset cluster keys. When required, use the CCM to reset the cluster key for every node in your deployment. New cluster keys are automatically used to wrap the cryptographic keys within the CMS repository.

8.13.1.1 To reset the cluster key on Windows

Prerequisites

Before resetting the cluster key for your node, make sure all servers managed by the Server Intelligence Agent are stopped.

Procedure

1. To launch the CCM, go to *Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *Central Configuration Manager*.
2. In the CCM, right-click the Server Intelligence Agent (SIA) and select *Stop*.

   > ⚠ Caution
   >
   > Do not proceed to step 3 until the SIA status is Stopped.

3. Right-click the Server Intelligence Agent (SIA) and select *Properties*.
   The *Properties* dialog box appears.
4. Click the *Configuration* tab.
5. Click *Change* under *CMS Cluster Key Configuration*.
   A warning message appears.
6. Click *Yes* to continue.
   The *Change Cluster Key* dialog box appears.
7. Enter the same eight-character key in the *New Cluster Key* and *Confirm New Cluster Key* fields.

   > ⓘ Note
   >
   > On Windows, cluster keys must contain a combination of uppercase and lowercase characters. Alternately, users can also generate a random key. A random key is required in order to be FIPS-compliant.

8. Click *OK* to submit the new cluster key to the system.
   A message appears, confirming that the cluster key was reset successfully.
9. Restart the SIA.

Results

Next Steps

In a multi-node cluster, you must reset the cluster keys for all the SIAs in your BI platform deployment to the new key.

8.13.1.2 To reset the cluster key on UNIX

Prerequisites

Before resetting the cluster key for a node, make sure all servers managed by the node have been stopped.

Procedure

1. Navigate to the `<INSTALLDIR>/sap_bobj` directory.
2. Type **`./cmsdbsetup.sh`** and press *Enter*.
   The *CMS Database Setup* screen appears.
3. Type the name of the node and press *Enter*.
4. Type **2** to change the cluster key.
   A warning message appears.
5. Select *Yes* to continue.
6. In the field provided, type a new cluster key and press *Enter*.

   > **Note**
   >
   > Make sure the key is at least six characters long, and combines two of the following character types: uppercase, lowercase, numbers or punctuation characters. For instance, you could have one lowercase character with a number, an uppercase character with a punctuation character, etc...

7. Re-enter the new cluster key in the field provided and press *Enter*.
   A message appears informing you that the cluster key has been successfully reset.
8. Restart the node.

Results

Next Steps

You must reset all the nodes in your BI platform deployment to use the same cluster key.

8.13.2 Cryptographic Officers

To manage cryptographic keys in the CMC you must be a member of the Cryptographic Officers group. The default administrator account created for the BI platform is also a member of the Cryptographic Officers group. Use this account to add users to the Cryptographic Officers group as required. It is recommended that membership to the group be restricted to a limited number of users.

> **Note**
>
> When users are added to the Administrators group, they do not inherit the rights required to perform management tasks on cryptographic keys.

8.13.2.1 To add a user to the Cryptographic Officers group

Prerequisites

A user account must exist in the BI platform before it can be added to the Cryptographic Officers group.

> ⓘ Note
>
> You must be a member of both the *Administrators* and *Cryptographic Officers* groups to add a user to the Cryptographic Officers group.

Procedure

1. In the *Users and Groups* management area of the CMC, select the *Cryptographic Officers* group.
2. Click *Actions* > *Add Members to Group*.
   The *Add* dialog box appears.
3. Click *User list*.
   The *Available Users or Groups* list refreshes and displays all user accounts in the system.
4. Move the user account that you want to add to the Cryptographic Officers group from the *Available Users or Groups* list to the *Selected Users or Groups* list.

   > → Tip
   >
   > To search for a specific user, use the search field.
5. Click *OK*.

Results

As a member of the Cryptographic Officers group, the newly added account will have access to the *Cryptographic Keys* management area in the CMC.

8.13.2.2 To view cryptographic keys in the CMC

Context

The CMC application contains a dedicated management area for cryptographic keys used by the BI platform system. Access to this area is restricted to members of the Cryptographic Officers group.

Procedure

1. To start the CMC, click *Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *SAP BusinessObjects BI platform Central Management Console*.
   The CMC home page appears.
2. Click the *Cryptographic Keys* tab.
   The *Cryptographic Keys* management area appears.
3. Double-click the cryptographic key for which you want to see further details.

Related Information

To view objects associated with a cryptographic key [page 166]

8.13.3 Managing cryptographic keys in the CMC

Cryptographic officers use the *Cryptographic Keys* management area to review, generate, deactivate, revoke, and delete keys used to protect sensitive data stored in the CMS repository.

All cryptographic keys currently defined in the system are listed on the *Cryptographic Keys* management area. Basic information for each key is provided under the headings described in the following table:

Heading	Description
Title	Name identifier of the cryptographic key
Status	The key's current status
Last Status Change	Date and time stamp for the last change associated with the cryptographic key
Objects	Number of objects associated with the key

Related Information

Cryptographic key status [page 165]
To create a new cryptographic key [page 166]
To delete a cryptographic key from the system [page 168]
To revoke a cryptographic key [page 168]
To view objects associated with a cryptographic key [page 166]
To mark cryptographic keys as compromised [page 167]

8.13.3.1 Cryptographic key status

The following table lists all the possible status options for cryptographic keys in the BI platform:

Status	Description
Active	Only one cryptographic key can be designated *Active* in the system. This key is used to encrypt current sensitive data that will be stored in the CMS database. The key is also used to decrypt all the objects that appear in its Object List. Once a new cryptographic key is created, the current *Active* reverts to the *Deactivated* state. An active key cannot be deleted from the system.
Deactivated	A *Deactivated* key can no longer be used to encrypt data. It can however be used to decrypt all the objects that appear in its Object List. You cannot reactivate a key once it has been deactivated. A key marked as *Deactivated* cannot be deleted from the system. You must change a key's status to *Revoked* before it can be deleted.
Compromised	A cryptographic key that is deemed to be insecure can be marked as compromised. By flagging such a key, you can later proceed to re-encrypt data objects that are still associated with the key. Once a key is marked as compromised it must be revoked before it can be deleted from the system.
Revoked	When a cryptographic key is revoked, a process is launched in which all objects currently associated with the key are re-encrypted with the current "Active" cryptographic key. Once a key is revoked it can safely be deleted from the system. The revocation mechanism ensures that data in the CMS database can always be decrypted. There is no way to reactivate a key once it has been revoked.
Deactivated: Rekeying-in process	Indicates that the cryptographic key is in the process of being revoked. Once the process is complete, the key will be marked as *Revoked*.
Deactivated: Rekeying-suspended	Indicates that the process for revoking a cryptographic key has been suspended. This usually occurs if the process has been deliberately suspended or if a data object associated with the key is not available.
Revoked-Compromised	A key is flagged as Revoked-Compromised if has been marked as compromised and all the data previously associated with it has been encrypted with another key. When a *Deactivated* key is marked as compromised, you are given a choice of not taking action or revoking the key. Once a compromised key is revoked it can be deleted.

8.13.3.2 To view objects associated with a cryptographic key

Procedure

1. Select the key in the *Cryptographic Keys* management area of the CMC.
2. Click *Manage* > *Properties*.
   The cryptographic key's *Properties* dialog box appears.
3. Click *Object List* in the navigation pane on the left of the *Properties* dialog box.
   All the objects associated with the cryptographic key are listed to the right of the navigation pane.

> → Tip
>
> Use the search functions to look for a specific object.

8.13.3.3 To create a new cryptographic key

Context

> ⚠ Caution
>
> When you create a new cryptographic key, the system automatically deactivates the current *Active* key. Once a key has been deactivated it cannot be restored as the *Active* key.

Procedure

1. In the *Cryptographic Keys* management area of the CMC, click *Manage* > *New* > *Cryptographic Key*.
   The *Create New Cryptographic Key* dialog box appears.
2. Click *Continue* to create the new cryptographic key.
3. Type the name and a description of the new cryptographic key; click *OK* to save your information.
   The new key is listed as the only active key in the *Cryptographic Keys* management area. The previously *Active* key is now marked as *Deactivated*.

Results

All new sensitive data generated and stored in the CMS database will now be encrypted with the new cryptographic key. You have the option to revoke the previous key and re-encrypt all its data objects with the new active key.

8.13.3.4 To mark cryptographic keys as compromised

Context

You can mark a cryptographic key as compromised if for some reason a cryptographic key is considered to no longer be secure. This is useful for tracking purposes and you can proceed to identify which data objects are associated with the key. A cryptographic key must be deactivated before it can marked as compromised.

> **Note**
>
> You can also mark a key as compromised after it has been revoked.

Procedure

1. Go to the *Cryptographic Keys* management area of the CMC.
2. Select the cryptographic key you want to mark as compromised.
3. Click *Actions* > *Mark As Compromised*.
   The *Mark As Compromised* dialog box appears.
4. Click *Continue*.
5. Select one of following options from the *Mark As Compromised* dialog:
   - *Yes*: Launches the process to re-encrypt all data objects that are associated with the compromised key.
   - *No*: The *Mark As Compromised* dialog box is closed and the cryptographic key is marked as *Compromised* in the *Cryptographic Keys* management area.

     > **Note**
     >
     > If you select *No*, sensitive data will continue to be associated with the compromised key. The compromised key will be used by the system to decrypt the associated objects.

Related Information

To revoke a cryptographic key [page 168]
Cryptographic key status [page 165]
To view objects associated with a cryptographic key [page 166]

8.13.3.5 To revoke a cryptographic key

Context

A deactivated cryptographic key can still be used by data objects associated with it. To break the association between the encrypted objects and the deactivated key, you must revoke the key.

Procedure

1. Select the key you want to revoke from the keys listed in the *Cryptographic Keys* management area.
2. Click *Actions* > *Revoke*.
   The *Revoke* dialog box appears.
3. Click *OK*.
   A process is launched to encrypt all the key's objects with the current active key. If the key is associated with many data objects, it will be marked as *Deactivated: Re-encryption in process* until the re-encryption process is complete.

Results

Once a cryptographic key is revoked, it can be safely removed from the system since no sensitive data objects require the key for decryption.

8.13.3.6 To delete a cryptographic key from the system

Prerequisites

Before you can delete a cryptographic key from the BI platform, you must ensure that no data objects in the system require the key. This restriction ensures that all sensitive data stored in the CMS repository can always be decrypted.

Context

After you have successfully revoked a cryptographic key, use the following instructions to delete the key from the system.

Procedure

1. Go to the *Cryptographic Keys* management area of the CMC.
2. Select the cryptographic key you want to delete.
3. Click *Manage* > *Delete*.
   The *Delete* dialog box appears.
4. Click *Delete* to remove the cryptographic key from the system.
   The deleted key is no longer displayed in the *Cryptographic Keys* management area of the CMC.

Results

> **Note**
>
> Once a cryptographic key is deleted from the system, it cannot be restored.

Related Information

To revoke a cryptographic key [page 168]
Cryptographic key status [page 165]

8.14 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with applicable data privacy regulations, it is necessary to consider compliance with industry-specific legislation in different countries. SAP provides specific features and functions to support compliance with regards to relevant legal requirements, including data protection. SAP does not give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, this information does not give any advice or recommendation with regards to additional features that would be required in particular IT environments. Decisions related to data protection must be made on a case-by-case basis, under consideration of the given system landscape and the applicable legal requirements.

> **Note**
>
> In the majority of cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion of personal data. SAP does not provide legal advice in any form. Definitions and other terms used in this document are not taken from any given legal source.

8.14.1 Glossary

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.
Deletion	The irreversible destruction of **personal data**.
Retention period	The period of time between the end of purpose (EoP) for a data set and when this data set is deleted subject to applicable laws. It is a combination of the residence period and the blocking period.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization (e.g. tax auditors).
Sensitive personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data, data concerning health or sex life or sexual orientation • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts

Term	Definition
Residence period	The period of time after the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Where-used check (WUC)	A process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.

8.14.2 User Consent

SAP applications ask for user consent before collecting any personal data. SAP BusinessObjects Business Intelligence Platform provides functionality that allows data subjects to give consent to collect and process their personal data. SAP assumes that the user, for example an SAP customer collecting data, has consent from its data subject (a natural person such as a customer, contact, or account), to collect or transfer data to the solution.

> **Note**
>
> *User Consent Message*
>
> This Product contains open or freely configurable entry fields, which are not intended for storing personal data without additional technical and organizational measures to safeguard data protection and privacy.

8.14.3 Information Report

Each person has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed. In SAP BusinessObjects Business Intelligence Platform, it is possible to display all information stored about a certain data subject.

For more details on how a user can access information stored about the data subject, refer 'Accessing your info' section in the *Fiorified Business Intelligence Launch Pad User Guide* on the SAP Help Portal.

> **Note**
>
> Locally stored documents are not protected by SAP BusinessObjects Business Intelligence Platform. Protection needs to be provided by the respective device management (e.g. access control, encryption, etc.).

8.14.4 Read Access Logging

Read Access Logging (RAL) is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy. These common questions might be of interest for an application that uses Read Access Logging:

- Who accessed the data of a given business entity, for example a bank account?
- Who accessed personal data, for example of a business partner?
- Which employee accessed personal information, for example religion?
- Which accounts or business partners were accessed by which users?

These questions can be answered using information about who accessed particular data within a specified time frame. Technically, this means that all remote API and UI infostructures (that access the data) must be enabled for logging.

The SAP BusinessObjects BI platform does not identify, process, or store sensitive personal data. Read accesses are, therefore, not logged by the BI platform.

8.14.5 Deletion of Personal Data

- Simplified Blocking and Deletion: In addition to compliance with the applicable data privacy regulations, it is necessary to consider compliance with industry-specific legislation in different countries. A typical potential scenario in certain countries is that personal data shall be deleted after the specified, explicit, and legitimate purpose for the processing of personal data has ended, but only as long as no other retention periods are defined in legislation, for example, retention periods for financial documents. Legal requirements in certain scenarios or countries also often require blocking of data in cases where the specified, explicit, and legitimate purposes for the processing of this data has ended, but the data has to be retained in the database due to other legally defined retention periods. In some scenarios, personal data also includes referenced data. Therefore, the challenge for deletion and blocking is to first handle referenced data and finally other data, such as business partner data.
- Deletion of personal data: The handling of personal data is subject to applicable laws related to the deletion of such data at the end of purpose (EoP). If there is no longer a legitimate purpose that requires the use of personal data, it must be deleted. When deleting data in a data set, all referenced objects related to that data set must be deleted as well. It is also necessary to consider industry-specific legislation in different countries in addition to general data protection laws. After the expiration of the longest retention period, the data must be deleted.

Deleting Personal Data in SAP BusinessObjects BI Platform

SAP BusinessObjects BI platform and its clients do not identify or categorize data (acquired from data sources for analysis and reporting) into personal data. For such data, the information retrieval and transparency requirement needs to be managed by data-owning system. Erasure of data is a standard functionality of the data-owning system. Additionally, SAP BusinessObjects BI platform and its clients provide functionalities (live connectivity to data sources) to keep data in sync with data owning system.

However, user data maintained in the system can be accessed by the users themselves or by users authorized to manage this data for them. Users imported from Identity Providers (like Windows AD, LDAP etc) are kept in sync with them and need to be maintained in the Identity Provider itself.

Enterprise users created in the SAP BusinessObjects BI platform can be deleted or disabled by users authorized to manage this data for them. In this case, retention can be handled by just disabling the users in the system, and after the retention period these users can be deleted from the system manually by the users authorized to manage this data for them.

When you delete a user account, the Favorites folder, personal categories, and inbox for that user are deleted as well. The ownership of the artifacts in the public folder will be transferred from deleted user to Administrator. Note that for the disabled user, this needs to be done manually by the users authorized to manage this data for them.

The user object identifier is stored in audit database and commentary database, as well. However, this is not cleared on deletion of users as the user ID in audit logs is necessary for legal and security requirements. Similarly, comments made by user are for business purposes and hence need to be retained for conversational history. Comments are not expected to contain personal data as user is informed in advance not to maintain personal data in open fields.

Also, both audit and commentary database entries can be manually deleted by the authorized users.

For further details on how to disable a user, refer To modify a user account [page 91].

For further details on how to delete commentary entries made by a user, refer Managing BI Commentary Application Settings [page 657]

8.14.6 Change Log

Change Log in SAP BusinessObjects Business Intelligence Platform processes personal data of business partners that are involved in change requests and activities. If any changes are made regarding the business partner, the system logs the following information on personal data per change request and activity:

- User who has changed data
- Data and time of the change
- The change type (update, insert, deletion, single field documentation)
- The identifying keys and their values of the data records
- The old and new value of the attribute that has changed
- The heading name for the attribute that has been changed

You can define the fields to be logged.

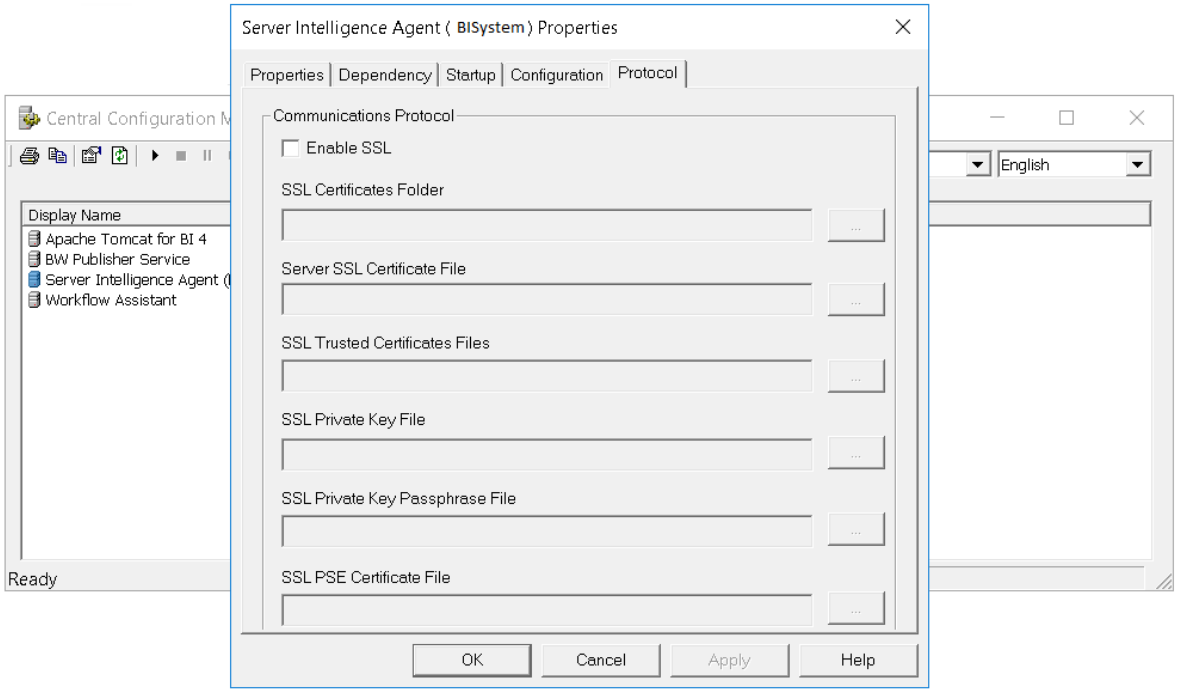
For further details on logs for user account update, refer Event Type ID: 1007 in Audit events and details [page 835].

8.15 Configuring backend servers for SSL

You can use the Secure Sockets Layer (SSL) protocol for all network communication between BI clients and BI servers in your BI platform deployment.

To set up SSL for all server communication, you need to perform the following steps:

- Deploy the BI platform with SSL enabled.
- Create key and certificate files for each machine in your deployment.
- Configure the location of these files in the Central Configuration Manager (CCM) and your web application server.
- You can also configure SSL for certificates that are either self-signed or managed by a certificate authority.



Note

If you are using thick clients, such as Crystal Reports, you also have to configure them for SSL if you are connecting to the CMS. Otherwise, you will get errors when you attempt to connect to a CMS that has been configured for SSL from a thick client that has not been configured in the same way.

8.15.1 To create the default configuration file

You can create a default configuration file to avoid repetitive addition of values during certificate or certificate signing request generation.

Context

> **Note**
>
> You must follow the below rules while creating the default configuration file.
>
> - You should add the values on the left-hand side exactly as mentioned below.
> - The values on left-hand side are case-sensitive.
> - There should be only one space between a value and the 'equal to' (=) sign. For example, there is only one space between *CA_Common_Name* and 'equal to' sign.
> - You must ensure there is no space after the values on the right-hand side.

Follow the steps below to create a default configuration file with the name **Name.cnf**:

Procedure

1. Open a new document in a text editor.
2. Add the values as given below:

```
CA_Common_Name = rootnm
CA_Country = DE
CA_State = BW
CA_Locality = RRR
CA_Email = example@example.com
CA_Unit = root_u
CA_Expiration[YYMMDD] = yymmdd
User_Expiration[YYMMDD] = yymmdd
User_Country = IN
User_State = KA
User_Locality = BLR
User_Organization = SSS
User_Unit = Unit
User_Common_Name = UserName
```

3. Save the file with the name **Name.cnf** at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows and `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` in Unix environment.

8.15.2 Creating key and certificate files

To set up SSL protocol for your server communication, use the GENPSE command line tool to create a key file and a certificate file for each machine in your deployment.

> **Note**
>
> You need to recreate the certificates for all machines in the deployment, including machines running thick client components such as Crystal Reports. For these client machines, use the `sslconfig` command line tool to do the configuration.

> **Note**
>
> For maximum security, all private keys should be protected and should not be transferred through unsecured communication channels.

8.15.2.1 To create key and certificate files for a machine

Context

This section covers the generation of self-signed key and certificates that are required to secure communications between servers, or server and client. You can generate the certificates using GENPSE tool, a command-line tool for executing numerous tasks related to Public Key Infrastructure. The GENPSE tool is used to generate X.509 certificates, certificate signing requests, and PSE files that are used in the CORBA SSL workflow. It is based on SAP's cryptographic library **CommonCryptoLib** and supports SHA-2 hasing mechanism.

Follow the steps below to create the required certificates for secure communication:

> **Note**
>
> You can create a default configuration file **Name.cnf** with the default values of the information requested while generating certificates. The default configuration file relieves you from repetitive addition of details for each certificate. Refer To create the default configuration file [page 175] for more information.

Procedure

1. Go to `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows and `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` in Unix.
2. Run the command:
   - In Windows: `GenPSE.exe selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`
   - In Unix: `GenPSE.sh selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`

Refer the table below for understanding the command:

Command	Function
GenPSE.exe or GenPSE.sh	Start the cryptography tool
selfsigned	To generate self-signed certificates
<Name.pse>	Server PSE filename
<Name.der>	Server Certificate filename
<root Cert.der>	Certificate Authority certificate name
<Name.key>	Server private key filename
<private key password.txt>	Passphrase for server private key file
< path to Name.cnf >	File path of the default configuration file

3. Enter the following details to generate Root Certificate Authority, Server, and Client Certificate.
   - *Country Name*
   - *State or Province Name*
   - *Locality Name*
   - *Organization Name*
   - *Organizational Unit Name*
   - *Enter your Name*
   - *Common Name*
   - *Email Address*
   - *Enter Expiration Date in YYMMDD format*
4. Your PSE file and the certificates are generated and stored at`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows and `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` in Unix.

> → Tip
>
> While generating user certificate, there is an additional parameter *User Certificate type* that allows the tool to identify and create the certificate for server or client authentication. Currently, any choice made under this parameter has no impact on the CORBA SSL setup.

> ⓘ Note
>
> - Server PSE and Certificate Authority certificate file should have different names.
> - The expiration date is supported till 2049.

8.15.3 Setting up SSL when the certificate is managed by a certificate authority

Context

You should generate a certificate signing request for a third-party certificate authority to sign the certificates. GenPSE tool generates a certificate signing request by executing simple commands and providing necessary information when prompted.

Follow the steps below to generate a certificate signing request:

> **Note**
>
> You can create a default configuration file `Name.cnf` with the default values of the information requested while generating certificates. The default configuration file relieves you from repetitive addition of details for each certificate. Refer To create the default configuration file [page 175] for more information.

Procedure

1. Go to `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows and`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` in Unix.
2. Run the command:
   - In Windows: `GenPSE.exe gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`
   - In Unix: `GenPSE.sh gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`

Command	Function
GenPSE.exe or GenPSE.sh	Start the cryptography tool
gencsr	To generate Certificate Signing Request
<csrname.p10>	Certificate Signing Request filename
<Name.key>	Server private key filename
<private key password.txt>	Passphrase for server private key file
<path to Name.cnf>	Path of the default configuration file

3. Enter the following information:
   - *Enter private key passphrase to set*
   - *Re-enter private key passphrase to confirm*
   - *Country Name*
   - *State or Province Name*

- *Locality Name*
- *Organizational Unit Name*
- *Common Name*
- *Email Address*

4. Your CSR file in p10 format, server private key, and the passphrase file are generated and stored at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows and`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` in Unix. The generated CSR file is sent to the certificate authority to generate a signed certificate.

8.15.3.1 Generating a pse File

Context

When your certificates are managed by an external certificate authority, you should generate a PSE file. Follow the steps below to generate a PSE file:

Procedure

1. Open `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Launch command line console and run `set SECUDIR=.` for Windows and `export SECUDIR=.` for Linux.
3. Run `sapgenpse import_p8 -p <file_path_PSE> -c <file_path_server_certificate> -r <file_path_CA_certificate> -z <file_path_passphrase_text_file> <file_path_server_key>`.

   Refer the table below for better understanding of the command:

Command	Description
sapgenpse	Start the cryptography tool
import_p8	Create a new PSE file from a PKCS#8 format private key (optionally protected by PKCS#5 password-based encryption) along with all necessary X.509 certificates
-p <file_path_PSE>	File path to the new PSE file that is created
-c <file_path_server_certificate>	File path to the server certificate
-r <file_path_CA_certificate>	File path to the CA certificate

Command	Description
-z <file_path_passphrase_text_file>	File path to the passphrase text file
<file_path_server_key>	File path to the server private key file

Example

sapgenpse import_p8 -p C:\SSL\cert.pse -c C:\SSL\servercert.der -r C:\SSL\cacert.der -z C:\SSL\passphrase.txt C:\SSL\server.key

4. Provide an empty password by pressing enter on password prompt.
5. Add the user credentials to the created pse file.

Tip

If SIA is running with LocalSystem account, then you have to execute the following command: `sapgenpse seclogin -p C:\SSL\cert.pse -O SYSTEM` to add the user credentials in the pse file.

Note

You can use any name of your choice for the pse file.

8.15.4 Configuring the SSL protocol

After you create keys and certificates for each machine in your deployment, and store them in a secure location, you need to provide the Central Configuration Manager (CCM) and your web application server with the secure location.

You also need to implement specific steps for configuring the SSL protocol for the web application server and for any machine running a thick-client application.

Enable FIPS in Unix-based Platform for Configuring SSL

FIPS is enabled by default for a complete installation of 4.2 SP04 or higher but you should enable it manually for scenarios mentioned below:

- Patch update from 4.1 SPXX to 4.2 SP04
- Patch Update from 4.1 SPXX to 4.2 SP02 or SP03 and later updating to 4.2 SP04

Note

In Windows, CORBA SSL works even when FIPS is not enabled whereas in Unix-based platforms, it is necessary to ensure that FIPS is enabled for servers before configuring CORBA SSL.

Steps to enable FIPS:

- Go to `<INSTALLDIR>/sap_bobj.`
- Run `./stopservers`
- Open ccm.config file.
- Add the text '-FIPS' from the SIA Node property list.
- Run `./startservers`

8.15.4.1 To configure the SSL protocol in the CCM

Procedure

1. In the CCM, right-click the Server Intelligence Agent and choose *Properties*.
2. In the Properties dialog box, click the *Protocol* tab.
3. Make sure *Enable SSL* is selected.
4. Provide the file path for the directory where you stored the key and certificate files.

Field	Description
SSL Certificates Folder	Folder where all the required SSL certificates and files are stored. For example: `d:\ssl`
Server SSL Certificate File	Name of the file used to store the server SSL certificate. By default, `servercert.der`
SSL Trusted Certificates File	Name of the file with the SSL trusted certificate. By default, `cacert.der`
SSL Private Key File	Name of the SSL private key file used to access the certificate. By default, `server.key`
SSL Private Key Passphrase File	Name of the text file containing the passphrase used to access the private key. By default, `passphrase.txt`
SSL Pse Certificate File	Name of the pse file that contains information about the trusted and server certificates.

> **Note**
>
> Make sure you provide the directory for the machine that the server is running on.

8.15.4.2 To configure the SSL protocol on Unix

Context

You must use the `serverconfig.sh` script to configure the SSL protocol for a SIA. This script provides a text-based program that enables you to view server information and to add and delete servers from your installation. The `serverconfig.sh` script is installed on the `sap_bobj` directory in your installation.

Procedure

1. Use the `ccm.sh` script to stop the SIA and all SAP BusinessObjects servers.
2. Run the `serverconfig.sh` script.
3. Select *3 - Modify Node*, and press `Enter`.
4. Specify the target SIA, and press `Enter`.
5. Select *1 - Modify Server Intelligence Agent SSL configuration*.
6. Select *ssl*.
   When prompted, specify the SSL certificate locations.
7. Repeat steps 1-6 for each SIA, if your BI platform deployment is a SIA cluster.
8. Start the SIA with the `ccm.sh` script, and wait for the servers to start.

8.15.4.3 To configure the SSL protocol for the web application server

Procedure

1. If you have a J2EE web application server, run the Java SDK with the following system properties set. For example:

   ```
   -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl
   -DtrustedCert=cacert.der -DsslCert=clientcert.der -DsslKey=client.key
   -Dpassphrase=passphrase.txt -Dpsecert=cert.pse
   ```

   The following table shows the descriptions that correspond to these examples:

Example	Description
`-DcertDir=d:\ssl`	The directory to store all the certificates and keys.
`-DtrustedCer=cacert.der`	Trusted certificate file. If specifying more than one, separate with semicolons.

Example	Description
`-DsslCert=clientcert.der`	Certificate used by the SDK.
`-DsslKey=client.key`	Private key of the SDK certificate.
`-Dpassphrase=passphrase.txt`	The file that stores the passphrase for the private key.
`-Dpsecert=cert.pse`	A PSE is a repository that contains keys and certificates used for securing communication. For more information, see 3026364

> **Note**
>
> For default web application server Tomcat, these properties are set in:
> - Linux / Unix: `INSTALLDIR/sap_bobj/tomcat/bin/setenv.sh`
> - Windows: `Tomcat Configuration -> Java -> Java Options`

2. If you have an IIS web application server, run the `sslconfig` tool from the command line and follow the configuration steps.

8.15.4.4 To configure thick clients

Prerequisites

Before performing the following procedure you need to create and save all the required SSL resources (for example, certificates and private keys) in a known directory.

Context

In the procedure below it is assumed that you have followed the instructions for creating the following SSL resources:

SSL resource	
SSL certificates folder	`d:\ssl`
Server SSL certificate file name	`servercert.der`
SSL trusted certificate or root certificate file name	`cacert.der`
SSL private key file name	`server.key`
File containing passphrase for accessing the SSL private key file	`passphrase.txt`

SSL resource	
SSL Pse Certificate File Name	cert.pse

Once the above resources have been created, use the following instructions to configure thick client applications such as the Central Configuration Manager (CCM).

Procedure

1. Make sure the thick-client application is not in operation.

   > **Note**
   >
   > Make sure you provide the directory for the machine that the server is running on.

2. Run the `sslconfig.exe` command line tool. Depending on your configuration, make sure you run the tool from win32_x86 for 32bit clients or win64_x64 for 64bit clients.

   The SSLC tool is installed with your BI platform software. (On Windows, for example, it is installed by default in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)

3. Type the following command:

   ```
   sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey
   server.key
   -passphrase     passphrase.txt -psecert cert.pse -protocol ssl
   ```

4. Restart the thick client application.

Related Information

To create key and certificate files for a machine [page 176]

8.15.4.4.1 To configure SSL login for the translation management tool

Context

To enable users to use SSL login with the translation management tool, information about the SSL resources must be added to the tool's configuration (`.ini`) file.

Procedure

1. Locate the `TransMgr.ini` file in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
2. Using a text editor, open the `TransMgr.ini`.
3. Add the following parameters:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<D:\SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Save the file and close the text editor.

Results

Users can now use SSL to log into the translation management tool.

8.15.4.4.2 To configure SSL for report conversion tool

RCT is being deprecated in BI 4.3 release. For more details, please refer to 2801797

8.16 Understanding communication between BI platform components

If your BI platform system is deployed entirely on the same secured subnet, there is no need to perform any special configuration of your firewalls. However, you might choose to deploy some components on different subnets separated by one or more firewalls.

It is important to understand the communication between BI platform servers, rich clients, and the web application server hosting the SAP BusinessObjects SDK before configuring your system to work with firewalls.

Related Information

Configuring the BI platform for firewalls [page 196]
Examples of typical firewall scenarios [page 201]

8.16.1 Overview of BI platform servers and communication ports

It is important to understand the BI platform servers and their communication ports if the system is deployed with firewalls.

8.16.1.1 Each BI platform server binds to a request port

A BI platform server, the Input File Repository Server for example, binds to a request port when it starts. Other BI platform components including servers, rich clients, and the SDK hosted in the web application server can use this request port to communicate with the server.

A server will select its request port number dynamically when the server starts or restarts, unless it is configured to use a specific port number. A specific request port number must be manually configured for servers that communicate with other BI platform components across a firewall.

8.16.1.2 Each BI platform server registers with the CMS

BI platform servers register with the CMS when they start. When a server registers, the CMS records:

- The hostname (or IP address) of the server's host machine.
- The server's Request Port number.

8.16.1.3 The CMS uses two ports

The CMS uses two ports: the Request Port and the Name Server Port. The Request Port is selected dynamically by default. The Name Server Port is 6400 by default.

All BI platform servers and client applications will initially contact the CMS™ on its Name Server port. The CMS™ will respond to this initial contact by returning the value of its Request Port. The servers will use this Request Port for subsequent communication with the CMS™.

8.16.1.4 Central Management Server (CMS) directory of registered services

The CMS provides a directory of the services that have registered with it. Other BI platform components such as web services, rich clients, and the SDK hosted in the web application server can contact the CMS and request a reference to a particular service. A service's reference contains the service's request port number and the host name (or IP address) of the server's host machine and service ID.

BI platform components might reside on a different subnet than the server they are using. The host name (or IP address) contained in the service's reference must be routable from the component's machine.

> **Note**
>
> The reference to a BI platform server will contain the server machine's host name by default. (If a machine has more than one host name, the primary host name is chosen). You can configure a server so that its reference contains the IP address instead.

Related Information

Communication between BI platform components [page 188]

8.16.1.5 Server Intelligence Agents (SIA) communicate with the Central Management Server (CMS)

Your deployment will not work if the Server Intelligence Agent (SIA) and Central Management Server (CMS) cannot communicate with each other. Ensure that your firewall ports are configured to allow communication between all SIAs and all CMSs in the cluster.

8.16.1.6 Job server child processes communicate with the data tier and the CMS

Most job servers create a child process to handle a task such as generating a report. The job server creates one or more child processes. Each child process has its own Request Port.

By default, a job server will dynamically select a Request Port for each child process. You can specify a range of port numbers that the job server can select from.

All child processes communicate with the CMS. If this communication crosses a firewall, you must:

- Specify the range of port numbers that the job server can select from by adding the `-requestJSChildPorts <lowestport>-<highestport>` and `-requestPort <port>` parameters to the server's command line. Note that the port range should be large enough to allow the maximum number of child process as specified by `-maxJobs`.
- Open the specified port range on the firewall.

Many child processes communicate with the data tier. For example, a child process might connect to a reporting database, extract data, and calculate values for a report. If the job server child process communicates with the data tier across a firewall, you must:

- Open a communicate path on the firewall from any port on the job server machine to the database listen port on the database server machine.

Related Information

Command lines overview [page 1014]

8.16.2 Communication between BI platform components

BI platform components, such as browser clients, rich clients, servers, and the SDK hosted in the web application server, communicate with each other across the network during typical workflows. You must understand these workflows to deploy SAP BusinessObjects products across different subnets that are separated by a firewall.

8.16.2.1 Requirements for communication between BI platform components

Deployments of the BI platform must conform to these general requirements.

1. Every server must be able to initiate communication with every other BI platform server on that server's Request Port.
2. The Central Management Server uses two ports. Every BI platform server, rich client, and the web application server that hosts the SDK must be able to initiate communication with the CMS on both of its ports.
3. Every job server child process must be able to communicate with the CMS.
4. Thick clients must be able to initiate communication with the Request Port of the Input and Output File Repository Servers.
5. If auditing is enabled for thick clients and web applications, they must be able to initiate communication with the request ports of the Adaptive Processing Servers that host the Client Auditing Proxy Service.
6. In general, the web application server that hosts the SDK must be able to communicate with the Request Port of every BI platform server.

   > **Note**
   >
   > The web application server only needs to communicate with BI platform servers that are used in the deployment. For example, if Crystal Reports is not being used, the web application server does not need to communicate with the Crystal Reports Cache Servers.

7. Job Servers use the port numbers that are specified with the `-requestJSChildPorts <lowestport>-<highestport>` command. If no range is specified in the command line, the servers use random port numbers. To allow a job server to communicate with a CMS, FTP, SFTP, or mail server on another machine open all of the ports in the range specified by `-requestJSChildPorts` on your firewall.
8. The CMS must be able to communicate with the CMS database listen port.
9. The Connection Server, most Job Server child process, and every system database and auditing Processing Server must be able to initiate communication with the reporting database listen port.

Related Information

BI platform port requirements [page 189]

8.16.2.2 BI platform port requirements

This section lists the communication ports used by BI platform servers, thick clients, the web application server hosting the SDK, and third-party software applications. If you deploy the BI platform with firewalls, you can use this information to open the minimum number of ports in those firewalls.

8.16.2.2.1 Port Requirements for BI platform applications

This table lists the servers and port numbers used by BI platform applications.

Product	Client Application	Associated Servers	Server Port Requirements
Crystal Reports	SAP Crystal Reports 2025 designer	CMS	CMS Name Server Port (6400 by default)
		Input FRS	CMS Request Port
		Output FRS	Input FRS Request Port
		Crystal Reports 2025 Report Application Server (RAS)	Output FRS Request Port
		Crystal Reports 2025 Processing Server	Crystal Reports 2025 Report Application Server Request Port
		Crystal Reports Cache Server	Crystal Reports 2025 Processing Server Request Port
			Crystal Reports Cache Server Request Port
SAP Analysis for Microsoft Office	SAP Analysis for Microsoft Office	CMS	CMS Name Server Port (6400 by default)
		Adaptive Processing Server hosting the Multi-Dimensional Analysis Service	CMS Request Port
			Adaptive Processing Server Request Port
		Input FRS	Input FRS Request Port
		Output FRS	Output FRS Request Port
BI platform	SAP BusinessObjects Web Intelligence Rich Client	CMS	CMS Name Server Port (6400 by default)
		Input FRS	CMS Request Port
			Input FRS Request Port

Product	Client Application	Associated Servers	Server Port Requirements
BI platform	Business View Manager	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port
BI platform	Central Configuration Manager (CCM)	CMS Server Intelligence Agent (SIA)	The following ports must be open to allow CCM to manage remote BI platform servers: CMS Name Server Port (6400 by default) CMS Request Port The following ports must be open to allow CCM to manage remote SIA processes: Microsoft Directory Services (TCP port 445) NetBIOS Session Service (TCP port 139) NetBIOS Datagram Service (UDP port 138) NetBIOS Name Service (UDP port 137) DNS (TCP/UDP port 53) (Note that some ports listed above may not be required. Consult your Windows administrator).
BI platform	Server Intelligence Agent (SIA)	Every BI platform server including the CMS	SIA Request Port (6410 by default) CMS Name Server Port (6400 by default) CMS Request Port
BI platform	Repository Diagnostic Tool	CMS Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port
BI platform	BI platform SDK hosted in the web application server	All BI platform servers required by the deployed products. For example, communication with the Crystal Reports 2025 Processing Server Request Port is required if the SDK is retrieving and interacting with Crystal reports from the CMS.	CMS Name Server Port (6400 by default) CMS Request Port Request Port for each server that is required. For example, the Crystal Reports 2025 Processing Server Request Port.

Product	Client Application	Associated Servers	Server Port Requirements
BI platform	Web Services provider (`dswsbobje.war`)	All BI platform servers required by the products accessing the web services. For example, communication with the Dashboards Cache and Processing Server Request Ports is required if SAP BusinessObjects Dashboards is accessing Enterprise data source connections through the Web Services provider.	CMS Name Server Port (6400 by default) CMS Request Port Request Port for each server that is required. For example, the Dashboards Cache Server and Dashboards Processing Server Request Ports.

8.16.2.2.2 Port Requirements for Third-Party Applications

This table lists third-party software used by SAP BusinessObjects products. It includes specific examples from some software vendors, but different vendors will have different port requirements.

Third-party application	SAP BusinessObjects component that uses the third-party product	Third-party application port requirement	Description
CMS System Database	Central Management Server (CMS)	Database server listen port	The CMS is the only server that communicates with the CMS system database.
CMS Auditing Database	Central Management Server (CMS)	Database server listen port	The CMS is the only server that communicates with the CMS auditing database.
Reporting Database	Connection Server Every Job Server child process Every Processing Server	Database server listen port	These servers retrieve information from the reporting database.
web application server	All SAP BusinessObjects web services and web applications including BI launch pad and CMC	HTTP port and HTTPS port. For example, on Tomcat the default HTTP port is 8080 and the default HTTPS port is 443.	The HTTPS port is only required if secure HTTP communication is used.
FTP server	Every Job Server	FTP In (port 21) FTP Out (port 22)	The Job Servers use the FTP ports to allow *send to FTP*.

Third-party application	SAP BusinessObjects component that uses the third-party product	Third-party application port requirement	Description
SFTP server	Every Job Server	SFTP (port 22)	The Job Servers use the SFTP ports to allow *send to SFTP*. **Note** A host key fingerprint is used to secure an SSH connection and prevents man-in-the-middle attacks. It is a mandatory non null parameter required to configure SFTP. The process to generate the host key fingerprint varies depending on the SFTP server used. The Administrator/User needs to configure SHA-2 fingerprint to enable SFTP. The Administrator/User can refer to the product documentation of their SSH/SFTP server implementations to generate an SHA-2 fingerprint. **Example** Common SFTP clients, such as PuTTY and WinSCP, use MD5 fingerprints to uniquely identify SFTP servers. MD5 fingerprints do not work. Refer to the SFTP server documentation for instructions on how to retrieve SHA-2 fingerprints. A sample method, given a public key file, and OpenSSH Unix tools, is described below. Given a public key file named RSAKey.pub that contains: `ssh-rsa <base64 encoded key>`, execute the following script: `cut -d ' ' -f 2 < RSAKey.pub | base64 -d | openssl dgst -c -sha256`. that outputs, for example: `(stdin)= 00:93:1e:cc:bd:cc:43:0`

Third-party application	SAP BusinessObjects component that uses the third-party product	Third-party application port requirement	Description
			`5:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8`, where the 20-digit digest depends on the value of the base64 encoded public key. Use the 20-digit value `00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8` for the host key fingerprint. → Recommendation The recommended best practice is to enable SFTP configuration in the servers page of the CMC in BOE and use default settings when sending across to SFTP servers.

Third-party application	SAP BusinessObjects component that uses the third-party product	Third-party application port requirement	Description
Email server	Every Job Server	SMTP (port as per SMTP Server)	You can use the same port for SMTPS and SMTP. However, for SMTPS, ensure that the server has SSL/TLS enabled using the STARTTLS smtp command. The Job Servers use the SMTP port to allow *send to email*. **Configuring Adaptive Job Server:** To configure the Adaptive Job Server, follow the below mentioned steps: 1. Launch the Central Management Console (CMC) 2. Choose *Servers* from the drop down. 3. Right-click on **AdaptiveJobServer** and choose *Destination* 4. Choose *Email* from the drop down. If you haven't already added Email server as a destination, then you need first add Email server as a destination before you proceed. 5. Enter the necessary details. 6. Check the *Enable SSL* option if required. 7. Choose *Save and Close*. **Setting up SMTP over SSL:** To setup SMTP over SSL, it is required that the SMTP server certificate be present in the Server and the BOE system. To setup SMTP over SSL, follow the below mentioned steps: 1. Generate certificate from SMTP server. 2. In the *Destination* window, check the *Enable SSL* checkbox.

Third-party application	SAP BusinessObjects component that uses the third-party product	Third-party application port requirement	Description
			3. Enter the absolute path to the SMTP certificate. **Note** Enter an absolute path to the SMTP certificate. If you do not enter an absolute path to the SMTP certificate, you can enter a placeholder (%SI_DEFAULT_CERT_LOC%) and the system reads this as the default location i.e. `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\` or `\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` and looks for the certificate (default name of the certificate is certificate.crt). 4. Select the desired *Connection Security*. **Note** By default, *StartTLS* option is selected. You can choose to select *SSL/TLS*. 5. Select the desired TLS version. **Note** By default, TLS v1.0 is selected. You can choose to select TLS v1.1 or TLS v1.2. 6. Choose *Save & Close*. SMTP over SSL is now setup.

Third-party application	SAP BusinessObjects component that uses the third-party product	Third-party application port requirement	Description
			Note When you perform a patch update from BI 4.1 SP6 to any higher version, by default, StartTLS option, and TLS v1.0 is selected.
			Note • When the user checks the *Enable SSL* checkbox, a secure channel is enabled. This allows secure SMTP communication over SSL. • You can configure only one SMTP Certificate per Adaptive Job Server. You cannot have multiple certificates configured for one job server. • *Enable SSL* option is available only in the Adaptive Job Server and not at the document level.
Unix servers to which the Job Servers can send content	Every Job Server	rexec out (port 512) (Unix only) rsh out (port 514)	(Unix only) The Job Servers use these ports to allow send to disk.
Authentication Server	CMS™ web application server that hosts the SDK every thick Client, for example Live Office.	Connection port for third-party authentication. For example, the connection server for the Oracle LDAP server is defined by the user in the file ldap.ora.	User credentials are stored in the third-party authentication server. The CMS™, SDK, and the thick clients listed here need to communicate with the third-party authentication server when a user logs on.

8.17 Configuring the BI platform for firewalls

This section gives step-by-step instructions for configuring your BI platform system to work in a firewalled environment.

8.17.1 To configure the system for firewalls

Procedure

1. Determine which BI platform components must communicate across a firewall.
2. Manually configure the request port for each BI platform server that must communicate across a firewall.
3. Configure a port range for any job server children that must communicate across a firewall by adding the `-requestJSChildPorts <lowestport>-<highestport>` and `-requestPort <port>` parameters to the server's command line.
4. Configure the firewall to allow communication to the request ports and job server port range on the BI platform servers that you configured in the previous step.
5. (Optional) Configure the hosts file on each machine that hosts a BI platform server that must communicate across a firewall.

Related Information

Communication between BI platform components [page 188]
Configuring port numbers [page 451]
Command lines overview [page 1014]
Specifying the firewall rules [page 197]
Configure the hosts file for firewalls that use NAT [page 198]

8.17.1.1 Specifying the firewall rules

Context

You must configure the firewall to allow the necessary traffic between BI platform components. Consult your firewall documentation for details of how to specify these rules.

Specify one inbound access rule for each communication path that crosses the firewall. You might not need to specify an access rule for every BI platform server behind the firewall.

Use the port number you specify in the server *Request Port* box on the server's Properties page in the CMC. Remember that each server on a machine must use a unique port number. Some SAP BusinessObjects servers use more than one port.

> **Note**
>
> If the BI platform is deployed across firewalls that use NAT, every server on all machines needs a unique Request Port number. That is, no two servers in the entire deployment can share the same Request Port.

> **Note**
>
> You do not need to specify any outbound access rules. BI platform servers do not initiate communication to the web application server, or to any client applications. BI platform servers can initiate communication to

other platform servers in the same cluster. Deployments with clustered servers in an outbound-firewalled environment are not supported.

Example

This example shows the inbound access rules for a firewall between the web application server and the BI platform servers. In this case you would open two ports for the CMS, one port for the Input File Repository Server (FRS), and one port for the Output FRS. The Request Port numbers are the port numbers you specify in the *Request Port* box on the CMC configuration page for a server.

Source Computer	Port	Destination Computer	Port	Action
web application server	Any	CMS	6400	Allow
web application server	Any	CMS	<Request Port number>	Allow
web application server	Any	Input FRS	<Request Port number>	Allow
web application server	Any	Output FRS	<Request Port number>	Allow
Any	Any	CMS	Any	Reject
Any	Any	Other platform servers	Any	Reject

Related Information

Communication between BI platform components [page 188]

8.17.1.2 Configure the hosts file for firewalls that use NAT

This step is required only if the BI platform servers must communicate across a firewall on which Network Address Translation (NAT) is enabled. This step allows the client machines to map a server's hostname to a routable IP address.

> ⓘ Note
>
> The BI platform can be deployed on machines that use Domain Name System (DNS). In this case, the server machine host names can be mapped to externally routable IP address on the DNS server, instead of in each machine's `hosts` file.

Understanding Network Address Translation

A firewall is deployed to protect an internal network from unauthorized access. Firewalls that use NAT will map the IP addresses from the internal network to a different address that is used by the external network. This address translation improves security by hiding the internal IP addresses from the external network.

BI platform components such as servers, thick clients, and the web application server hosting the SDK will use a service reference to contact a server. The service reference contains the hostname of the server's machine. This hostname must be routable from the BI platform component's machine. This means the `hosts` file on the component's machine must map the server machine's hostname to the server machine's external IP address. The server machine's external IP address is routable from external side of the firewall, whereas the internal IP address is not.

The procedure for configuring the `hosts` file is different for Windows and UNIX.

8.17.1.2.1 To configure the hosts file on Windows

Procedure

1. Locate every machine that runs a BI platform component that must communicate across a firewall on which Network Address Translation (NAT) is enabled.
2. On each machine located in the previous step, open the `hosts` file using a text editor like Notepad. The `hosts` file is located at `\Windows\System32\drivers\etc\hosts`.
3. Follow the instructions in the `hosts` file to add an entry for each machine behind the firewall that is running a BI platform server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

8.17.1.2.2 To configure the hosts file on Unix

Context

> **Note**
>
> Your UNIX operating system must be configured first to consult the hosts file to resolve domain names before consulting DNS. Consult your UNIX systems documentation for details.

Procedure

1. Locate every machine that runs a BI platform component that must communicate across a firewall on which Network Address Translation (NAT) is enabled.

2. Open the hosts file using an editor like `vi`. The `hosts` file is located in the following directory `\etc`
3. Follow the instructions in the `hosts` file to add an entry for each machine behind the firewall that is running a BI platform server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

8.17.2 Debugging a firewalled deployment

Context

If one or more of your BI platform servers do not work when your firewall is enabled, even though the expected ports have been opened on the firewall, you can use the event logs to determine which of the servers is attempting to listen on which ports or IP Addresses. You can then either open those ports on your firewall, or use the Central Management Console (CMC) to change the port numbers or IP addresses that these servers attempt to listen on.

Whenever a BI platform server starts, the server writes the following information to the Event Log for each request port that it attempts to bind to.

- *Server* - The name of the server and whether it successfully started.
- *Published Address(es)* - A list of IP Address and port combinations which are posted to the name service that other servers will use to communicate with this server.

If the server successfully binds to a port, the log file also displays *Listening on port(s)*, the IP Address and port that the server is listening on. If the server is unsuccessful in binding to the port, the log file displays *Failed to listed on port(s)*, the IP Address and port that the server attempts to listen on and fails.

When a Central Management Server starts, it also writes Published Address(es), Listening on port(s), and Failed To Listen On information for the server's Name Service Port.

> **Note**
>
> If the server is configured to use a port that is auto-assigned and to use a host name or IP Address that is invalid, the event log indicates that the server failed to listen on the host name or IP Address and port "0". If a specified host name or IP Address is invalid, the server will fail before the host operating system is able to assign a port.

Example

The following example shows the an entry for a Central Management Server that is successfully listening on two Request Ports and a Name Service Port.

```
Server mynode.cms1 successfully started.
Request Port :
     Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
     Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032,
10.90.172.216:8765
```

```
Name Service Port :
     Published Address(es): mymachine.corp.com:6400
     Listening on port(s):  [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400,
10.90.172.216:6400
```

8.17.2.1 To debug a firewalled deployment

Procedure

1. Read the event log to determine if the server is successfully binding to the port that you have specified.

   If the server was unable to successfully bind to a port, there is probably a port conflict between the server and another process that is running on the same machine. The *Failed to List On* entry indicates the port that the server is attempting to listen on. Run a utility such as netstat to determine which process that has taken the port, and then configure either the other process or the server to listen on another port.
2. If the server was able to successfully bind to a port, *Listening On* indicates which port the server is listening on. If a server is listening on a port and is still not working properly, either ensure that that port is open on the firewall or configure the server so that it listens on a port that is open.

Results

If all of the Central Management Servers in your deployment are attempting to listen to ports or IP Addresses that are not available, then the CMSs will not start and you will not be able to log on to the CMC. If you want to change the port number or IP Address that the CMS attempts to listen, you must use the Central Configuration Manager (CCM) to specify a valid port number or IP Address.

Related Information

Configuring port numbers [page 451]

8.18 Examples of typical firewall scenarios

This section provides examples of typical firewall deployment scenarios.

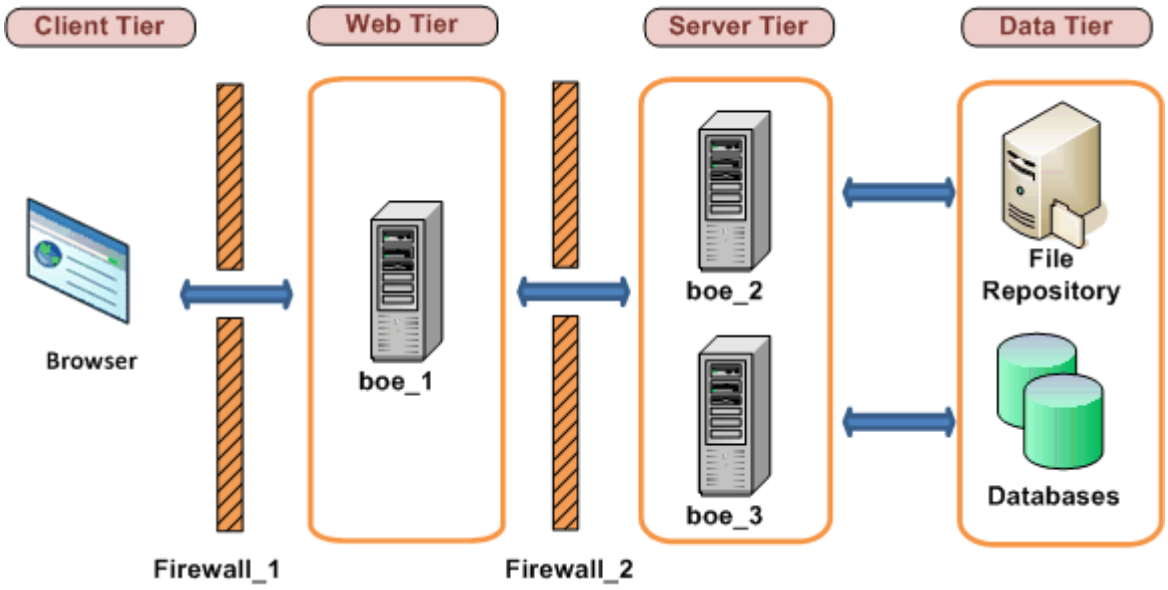
8.18.1 Example - Application tier deployed on a separate network

This example shows how to configure a firewall and the BI platform to work together in a deployment where the firewall separates the web application server from other BI platform servers.

In this example, BI platform components are deployed across these machines:

- Machine `boe_1` hosts the web application server and the SDK.
- Machine `boe_2` hosts the Intelligence tier servers, including the Central Management Server, the Input File Repository Server, the Output File Repository Server, and the Event server.
- Machine `boe_3` hosts the Processing tier servers, including the Adaptive Job Server, the Web Intelligence Processing Server, the Report Application Server, the Crystal Reports Cache Server, and Crystal Reports Processing Server.

Application tier deployed on a separate network



8.18.1.1 To configure an application tier deployed on a separate network

Context

The following steps explain how to configure this example.

Procedure

1. These communication requirements apply to this example:
   - The web application server that hosts the SDK must be able to communicate with the CMS on both of its ports.
   - The web application server that hosts the SDK must be able to communicate with every BI platform server.
   - The browser must have access to the http or the https Request Port on the Web Application Server.
2. The web application server must communicate with all BI platform servers on machine `boe_2` and `boe_3`. Configure the port numbers for each server on these machines. Note that you can use any free port between 1,025 and 65,535.
   The port numbers chosen for this example are listed in the table:

Server	Port Number
Central Management Server	6400
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event server	6425
Adaptive Job Server	6435
Crystal Reports Cache server	6440
Web Intelligence Processing Server	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. Configure the firewalls `Firewall_1` and `Firewall_2` to allow communication to the fixed ports on the servers and the web application server that you configured in the previous step.

   In this example we are opening the HTTP Port for the Tomcat Application server.

   Configuration for Firewall_1

Port	Destination Computer	Port	Action
Any	boe_1	8080	Allow

   Configuration for Firewall_2

Source Computer	Port	Destination Computer	Port	Action
boe_1	Any	boe_2	6400	Allow
boe_1	Any	boe_2	6411	Allow
boe_1	Any	boe_2	6415	Allow
boe_1	Any	boe_2	6420	Allow
boe_1	Any	boe_2	6425	Allow

Source Computer	Port	Destination Computer	Port	Action
boe_1	Any	boe_3	6435	Allow
boe_1	Any	boe_3	6440	Allow
boe_1	Any	boe_3	6460	Allow
boe_1	Any	boe_3	6465	Allow
boe_1	Any	boe_3	6470	Allow

4. This firewall is not NAT-enabled, and so we do not have to configure the `hosts` file.

Related Information

Configuring port numbers [page 451]
Understanding communication between BI platform components [page 185]

8.18.2 Example - Thick client and database tier separated from BI platform servers by a firewall

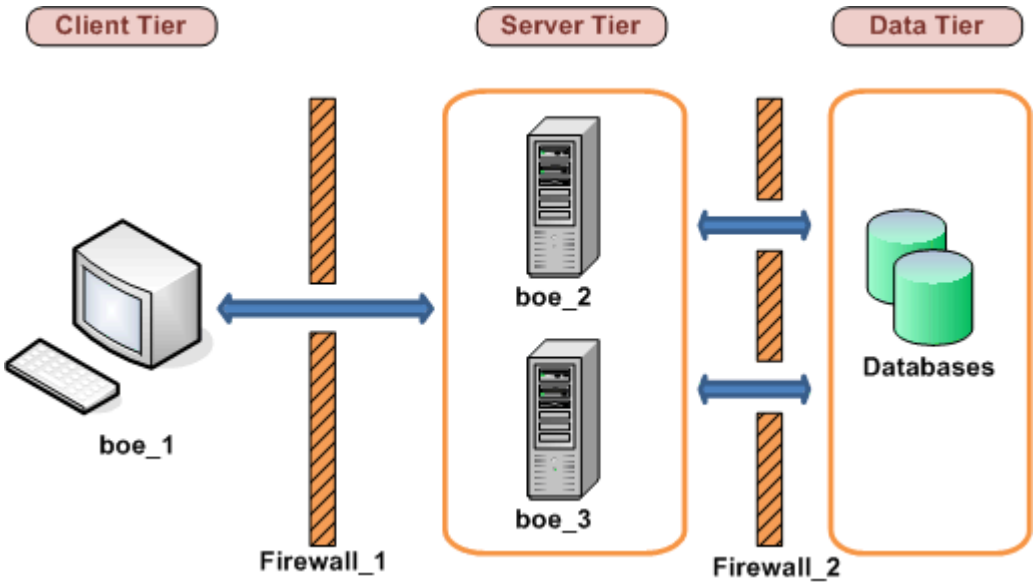
This example shows how to configure a firewall and the BI platform to work together in a deployment scenario where:

- One firewall separates a thick client from the BI platform servers.
- One firewall separates the BI platform servers from the database tier.

In this example, the BI platform components are deployed across these machines:

- Machine `boe_1` hosts the Publishing Wizard. Publishing Wizard is a BI platform thick client.
- Machine `boe_2` hosts the Intelligence tier servers, including the Central Management Server (CMS), the Input File Repository Server, the Output File Repository Server, and the Event server.
- Machine `boe_3` hosts the Processing tier servers, including: Adaptive Job Server, Web Intelligence Processing Server, Report Application Server, the Crystal Reports Processing Server, and Crystal Reports Cache Server.
- Machine `Databases` hosts the CMS system and auditing databases and the reporting database. Note that you can deploy both databases on the same database server, or you can deploy each database on its own database server. In this example, all the CMS databases and the reporting database are deployed on the same database server.

Rich client and database tier deployed on separate networks



8.18.2.1 To configure tiers separated from BI platform servers by a firewall

Context

The following steps explain how to configure this example.

Procedure

1. Apply the following communication requirements to this example:
   - The Publishing Wizard must be able to initiate communication with the CMS™ on both of its ports.
   - The Publishing Wizard must be able to initiate communication with the Input File Repository Server and the Output File Repository Server.
   - The Connection Server, every Job Server child process, and every Processing Server must have access to the listen port on the reporting database server.
   - The CMS™ must have access to the database listen port on the CMS™ database server.
2. Configure a specific port for the CMS™, the Input FRS, and the Output FRS. Note that you can use any free port between 1,025 and 65,535.
   The port numbers chosen for this example are listed in the table:

Server	Port Number
Central Management Server ™	6411
Input File Repository Server	6415

Server	Port Number
Output File Repository Server	6416

3. We do not need to configure a port range for the Job Server children because the firewall between the job servers and the database servers will be configured to allow any port to initiate communication.
4. Configure `<Firewall_1 >` to allow communication to the fixed ports on the platform servers that you configured in the previous step. Note that port 6400 is the default port number for the CMS™ Name Server Port and did not need to be explicitly configured in the previous step.

Port	Destination Computer	Port	Action
Any	boe_2	6400	Allow
Any	boe_2	6411	Allow
Any	boe_2	6415	Allow
Any	boe_2	6416	Allow

Configure `<Firewall_2 >`to allow communication to the database server listen port. The CMS™ (on *boe_2*) must have access to the CMS™ system and auditing database and the Job Servers (on *boe_3*) must have access to the system and auditing databases. Note that we did not have configure a port range for job server child processes because their communication with the CMS did not cross a firewall.

Source Computer	Port	Destination Computer	Port	Action
boe_2	Any	Databases	3306	Allow
boe_3	Any	Databases	3306	Allow

5. This firewall is not NAT-enabled, and so we do not have to configure the `hosts` file.

Related Information

Understanding communication between BI platform components [page 185]
Configuring the BI platform for firewalls [page 196]

8.19 Firewall settings for integrated environments

This section details specific considerations and port settings for BI platform deployments that integrate with the following ERP environments.

- SAP
- PeopleSoft

BI platform components include browser clients, rich clients, servers, and the SDK hosted in the Web Application server. System components can be installed on multiple machines. It is useful to understand the

basics of communication between the BI platform and the ERP components before configuring you system to work with firewalls

Port requirements for BI platform servers

The following ports are required for their corresponding servers in the BI platform:

Server Port Requirements
• Central Management Server Name Server port • Central Management Server Request port • Input FRS Request port • Output FRS Request port • Report Application Server Request port • Crystal Reports Cache Server Request port • Crystal Reports Page Server Request port • Crystal Reports Processing Server Request Port

8.19.1 Specific firewall guidelines for SAP integration

Your BI platform deployment must conform to the following communication rules:

- The CMS must be able to initiate communication with SAP system on SAP System Gateway port.
- The Adaptive Job Server and Crystal Reports Processing Server (along with Data Access components) must be able to initiate communication with SAP system on the SAP System Gateway port.
- The BW Publisher component must be able to initiate communication with the SAP system on the SAP System Gateway port.
- BI platform components deployed on the SAP Enterprise Portal side (for example, iViews and KMC) must be able to initiate communication with BI platform web applications on HTTP/HTTPS ports.
- The web application server must be able to initiate communication on the SAP System Gateway service.
- Crystal Reports must be able to initiate communication with the SAP host on the SAP System Gateway port and SAP System Dispatcher port.

The port that the SAP Gateway service is listening on is the same as that specified in the installation.

> ⓘ Note
>
> If a component requires an SAP router to connect to an SAP system, you can configure the component using the SAP router string. For example, when configuring an SAP entitlement system to import roles and users, the SAP router string can be substituted for the application server's name. This insures that the CMS will communicate with the SAP system through the SAP router.

Related Information

Installing a local SAP Gateway [page 937]

8.19.1.1 Detailed port requirements

Port requirements for SAP

The BI platform uses the SAP Java Connector (SAP JCO) to communicate with SAP NetWeaver. You need to configure and ensure the availability of the following ports:

- SAP Gateway service listening port (for example, 3300).
- SAP Dispatcher service listening port (for example, 3200).

The following table summarizes the specific port configurations that you need.

Source computer	Port	Destination computer	Port	Action
SAP	Any	BI platform Web Application Server	Web Service HTTP/ HTTPS port	Allow
SAP	Any	CMS	CMS Name Server port	Allow
SAP	Any	CMS	CMS Requested port	Allow
Web Application Server	Any	SAP	SAP System Gateway Service port	Allow
Central Management Server (CMS)	Any	SAP	SAP System Gateway Service port	Allow
Crystal Reports™	Any	SAP	SAP System Gateway Service port and SAP System Dispatcher port	Allow

8.19.2 Firewall configuration for JD Edwards EnterpriseOne integration

Deployments of the BI platform that will communicate with JD Edwards software must conform to these general communication rules:

- Central Management Console Web Applications must be able to initiate communication with JD Edwards EnterpriseOne through the JDENET port and a randomly selected port.
- Crystal Reports with Data Connectivity client side component must be able to initiate communication with JD Edwards EnterpriseOne through the JDNET port. For retrieving data, JD Edwards EnterpriseOne side must be able to communicate with the driver through a random port that cannot be controlled.

- Central Management Server must be able to initiate communications with JD Edwards EnterpriseOne through the JDENET port and a randomly selected port.
- The JDENET port number can be found in the JD Edwards EnterpriseOne Application Server configuration file (`JDE.INI`) under the JDENET section.

Port Requirements for BI platform servers

Product	Server Port Requirements
SAP BusinessObjects Business Intelligence platform	BI platform Sign-on Server port

Port Requirements for JD Edwards EnterpriseOne

Product	Port Requirement	Description
JD Edwards EnterpriseOne	JDENET port and a randomly selected port	Used for communication between the BI platform and the JD Edwards EnterpriseOne application server.

Configuring the web application server to communicate with JD Edwards

This section shows how to configure a firewall and the BI platform to work together in a deployment scenario where the firewall separates the web application server from other platform servers.

For firewall configuration with BI platform servers and clients, see the *BI platform port requirements* section of this guide. In addition to the standard firewall configuration, communication with JD Edwards servers requires some extra ports to be opened.

For JD Edwards EnterpriseOne Enterprise

Source Computer	Port	Destination Computer	Port	Action
CMS with Security Connectivity feature for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
BI platform servers with Data Connectivity for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
Crystal Reports with client side Data Connectivity for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
Web application server	Any	JD Edwards EnterpriseOne	Any	Allow

8.19.3 Specific firewall guidelines for Oracle EBS

Your deployment of the BI platform must allow the following components to initiate communication with the Oracle database listener port:

- BI platform web components
- CMS (specifically the Oracle EBS security plugin)
- BI platform backend servers (specifically the EBS Data Access component)
- Crystal Reports (specifically the EBS Data Access component)

> **Note**
>
> The default value of the Oracle database listener port in all the above is 1521.

8.19.3.1 Detailed port requirements

In addition to the standard firewall configuration for the BI platform, some extra ports need to be opened to work in an integrated Oracle EBS environment:

Source Computer	Port	Destination Computer	Port	Action
Web application server	Any	Oracle EBS	Oracle database port	Allow
CMS with security connectivity for Oracle EBS	Any	Oracle EBS	Oracle database port	Allow
BI platform servers with server-side data connectivity for Oracle EBS	Any	Oracle EBS	Oracle database port	Allow
Crystal Reports with client-side data connectivity for Oracle EBS	Any	Oracle EBS	Oracle database port	Allow

8.19.4 Firewall configuration for PeopleSoft Enterprise integration

Deployments of the BI platform that will communicate with PeopleSoft enterprise must conform to the following general communication rules:

- The Central Management Server (CMS) with the Security Connectivity component must be able to initiate communication with the PeopleSoft Query Access (QAS) web service.
- BI platform servers with a Data Connectivity component must be able to initiate communication with the PeopleSoft QAS web service.
- The Crystal Reports with Data Connectivity client components must be able to initiate communication with the PeopleSoft QAS web service.
- The Enterprise Management (EPM) Bridge must be able to communicate with the CMS and the Input File Repository Server.

- The EPM Bridge must be able to communicate with the PeopleSoft database using an ODBC connection.

The web service port number is the same as the port specified in PeopleSoft Enterprise Domain name.

Port Requirements for BI platform servers

Product	Server Port Requirements
SAP BI platform	BI platform Sign-on Server port

Port Requirements for PeopleSoft

Product	Port Requirement	Description
PeopleSoft Enterprise: People Tools 8.46 or newer	Web Service HTTP/HTTPS port	This port is required when using SOAP connection for PeopleSoft Enterprise for People Tools 8.46 and newer solutions

Configuring BI platform and PeopleSoft for firewalls

This section shows how to configure the BI platform and PeopleSoft Enterprise to work together in a deployment scenario where the firewall separates the Web Application server from other BI platform servers.

For firewall configuration with BI platform servers and clients, refer to the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

Besides the firewall configuration with the BI platform, you will need to do some extra configuration.

For PeopleSoft Enterprise: PeopleTools 8.46 or newer

Source Computer	Port	Destination Computer	Port	Action
CMS with Security Connectivity feature for PeopleSoft	Any	PeopleSoft	PeopleSoft web service HTTP /HTTPS port	Allow
BI platform servers with Data Connectivity for PeopleSoft	Any	PeopleSoft	PeopleSoft web service HTTP /HTTPS port	Allow
CrystalReports with client side Data Connectivity for PeopleSoft	Any	PeopleSoft	PeopleSoft web service HTTP /HTTPS port	Allow
EPM Bridge	Any	CMS	CMS Name Server Port	Allow
EPM Bridge	Any	CMS	CMS requested port	Allow
EPM Bridge	Any	Input File Repository Server	Input FRS port	Allow

Source Computer	Port	Destination Computer	Port	Action
EPM Bridge	Any	PeopleSoft	PeopleSoft Database Port	Allow

8.19.5 Firewall configuration for Siebel integration

This section shows which specific ports are used for communication between the BI platform and Siebel eBusiness Application systems when they are separated by firewalls.

- The Web Application must be able to initiate communication with the BI platform Sign-on Server for Siebel. For enterprise Sign-on Server for Siebel three ports are needed:
  1. The Echo (TCP) port 7 for checking access to the Sign-on Server.
  2. The BI platform Sign-on Server for Siebel port (By default 8448) for CORBA IOR listening port.
  3. A random POA port for CORBA communication that cannot be controlled, so all ports need to open.
- The CMS must be able to initiate communication with the BI platform Sign-on Server for Siebel. CORBA IOR listening port configured for each Sign-on Server (for example 8448). You will also need to open a random POA port number that will not be known until you have installed the BI platform.
- The BI platform Sign-on Server for Siebel must be able to initiate communication with SCBroker (Siebel connection broker) port (for example 2321).
- The BI platform backend servers (Siebel Data Access component) must be able to initiate communication with SCBroker (Siebel connection broker) port (for example 2321).
- Crystal Reports (Siebel Data Access component) must be able to initiate communication with SCBroker (Siebel connection broker) port (for example 2321).

Detailed description of ports

This section lists the ports that are used by the BI platform. If you deploy the BI platform with firewalls, you can use this information to open the minimum number of ports in those firewalls specific for integration with Siebel.

Port Requirements for BI platform servers

Product	Server Port Requirements
SAP BI platform	BI platform Sign-on Server port

Port Requirement for Siebel

Product	Port Requirement	Description
Siebel eBusiness Application	2321	Default SCBroker (Siebel connection broker) port

Configuring BI platform firewalls for integration with Siebel

This section shows how to configure firewalls for Siebel and the BI platform to work together in a deployment scenario where the firewall separates the Web Application server from other platform servers.

Source Computer	Port	Destination Computer	Port	Action
Web Application Server	Any	BI platform Sign-on Server for Siebel	Any	Allow
CMS	Any	BI platform Sign-on Server for Siebel	Any	Allow
BI platform Sign-on Server for Siebel	Any	Siebel	SCBroker port	Allow
BI platform servers with server side Data Connectivity for Siebel	Any	Siebel	SCBroker port	Allow
CrystalReports with client side Data Connectivity for Siebel	Any	Siebel	SCBroker port	Allow

8.20 The BI platform and reverse proxy servers

The BI platform can be deployed in an environment with one or more reverse proxy servers. A reverse proxy server is typically deployed in front of the web application servers in order to hide them behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, hiding private IP addresses.

Because the reverse proxy server translates the public URLs to internal URLs, it must be configured with the URLs of the BI platform web applications that are deployed on the internal network.

8.20.1 Understanding how web applications are deployed

BI platform web applications are deployed on a web application server. The applications are deployed automatically during installation through the WDeploy tool. The tool can also be used to manually deploy the applications after the BI platform is deployed. The web applications are located in the following directory on a default Windows installation:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps
```

WDeploy is used to deploy WAR files such as these:

- `BOE`: Includes the Central Management Console (CMC), BI launch pad, and Open Document
- `dswsbobje`: Contains the Web Services application

If the web application server is located behind a reverse proxy server, the reverse proxy server should be configured with the correct context paths of the WAR files. To expose all of the BI platform functionality, configure a context path for every BI platform WAR file that is deployed.

8.21 Configuring reverse proxy servers for BI platform web applications

The reverse proxy server must be configured to map incoming URL requests to the correct web application in deployments where BI platform web applications are deployed behind a reverse proxy server.

This section contains specific configuration examples for some of the supported reverse proxy servers. Refer to the vendor documentation for your reverse proxy server for more information.

8.21.1 Detailed instructions for configuring reverse proxy servers

Configure the WAR files

BI platform web applications are deployed as WAR files on a web application server. Ensure you configure a directive on your reverse proxy server for the WAR file that is required for your deployment. You can use WDeploy to deploy either the `BOE` or `dswsbobje` WAR files. For more information on WDeploy, see the *BI Platform Web Application Deployment Guide*.

Specify BOE properties in the custom configuration directory

The `BOE.war` file includes global and application specific properties. If you need to modify the properties, use the custom configuration directory. By default the directory is located at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> ⚠ Caution
>
> To avoid overwriting files in the default directory, do not modify the properties in the `config\default` directory. Users should use the `custom` directory.

> ⓘ Note
>
> On some web application servers, such as the Tomcat version bundled with the BI platform, you can access the `BOE.war` file directly. In such a scenario, you can set custom settings directly without undeploying the WAR file. When you cannot access the `BOE.war` file, you must undeploy, customize, and then redeploy the file.

Consistent use of forward slashes (/)

Define the context paths in the reverse proxy server in the same way as they are entered in a browser URL. For example, if the directive contains a forward slash (/) at the end of the mirror path on the reverse proxy server, enter a forward slash at the end of the browser URL.

Ensure the '/' character is used consistently in the source and destination URL in the directive of the reverse proxy server. If the '/' character is added at the end of the source URL, it must also be added to the end of the destination URL.

8.21.2 To configure the reverse proxy server

Context

The steps below are required for BI platform web applications to work behind a supported reverse proxy server.

Procedure

1. Ensure the reverse proxy server is set up correctly according to the vendor's instructions and the deployment's network topology.
2. Determine which BI platform WAR file is required.
3. Configure the reverse proxy server for each BI platform WAR file. Note that the rules are specified differently on each type of reverse proxy server.
4. Perform any special configuration that is required. Some web applications require special configuration when deployed on certain web application servers.

8.21.3 To configure Apache 2.2 reverse proxy server for the BI platform

Context

This section provides a workflow for configuring the BI platform and Apache 2.2 to work together.

Procedure

1. Ensure that the BI platform and Apache 2.2 are installed on separate machines.
2. Ensure that Apache 2.2 is installed and configured as a reverse proxy server as described in the vendor documentation.

3. Configure the `ProxyPass` for every WAR file that is deployed behind the reverse proxy server.
4. Open *httpd.conf* file that is located under the Apache Reverse proxy installation folder.
5. Configure the `ProxyPassReverseCookiePath` for every web application that is deployed behind the reverse proxy server. For example:

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.21.4 To configure WebSEAL 6.0 reverse proxy server for the BI platform

Context

This section explains how to configure the BI platform and WebSEAL 6.0 to work together.

The recommended configuration method is to create a single standard junction that maps all of the BI platform web applications hosted on an internal web application server or web server to a single mount point.

Procedure

1. Ensure that the BI platform and WebSEAL 6.0 are installed on separate machines.

   It is possible but not recommended to deploy the BI platform and WebSEAL 6.0 on the same machine. Refer to the WebSEAL 6.0 vendor documentation for instructions on configuring this deployment scenario.
2. Ensure that WebSEAL 6.0 is installed and configured as described in the vendor documentation.
3. Launch the WebSEAL *pdadmin* command line utility. Log in to a secure domain such as *sec_master* as a user with administration privileges.
4. Enter the following command at the *pdadmin sec_master* prompt:

   ```
   server task <instance_name-webseald-host_name> create -t
   <type> -h <host_name> -p <port> <junction_point>
   ```

   Where:

   - `<instance_name-webseald-host_name>` specifies the full server name of the installed WebSEAL instance. Use this full server name in the same format as displayed in the output of the `server list` command.
   - `<type>` specifies the type of junction. Use `tcp` if the junction maps to an internal HTTP port. Use `ssl` if the junction maps to an internal HTTPS port.
   - `<host_name>` specifies the DNS host name or IP address of the internal server that will receive the requests.

- `<port>` specifies the TCP port of the internal server that will receive the requests.
- `<junction_point>` specifies the directory in the WebSEAL protected object space where the document space of the internal server is mounted.

Example

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.21.5 To configure Microsoft ISA 2006 for the BI platform

Context

This section explains how to configure the BI platform and ISA 2006 to work together.

The recommended configuration method is to create a single standard junction that maps all of the BI platform WAR files hosted on an internal web application server or web server to a single mount point. Depending on your web application server, there are additional configuration required on the application server for it to work with ISA 2006.

Procedure

1. Ensure that the BI platform and ISA 2006 are installed on separate machines.

   It is possible but not recommended to deploy the BI platform and ISA 2006 on the same machine. Refer to the ISA 2006 documentation for instructions on configuring this deployment scenario.
2. Ensure that ISA 2006 is installed and configured as described in the vendor documentation.
3. Launch the ISA Server Management utility.
4. Use the navigation panel to launch a new publishing rule
   a. Go to

      Arrays > *MachineName* > *Firewall Policy* > *New* > *Web Site Publishing Rule*

      > → Remember
      >
      > Replace `MachineName` with the name of the machine on which ISA 2006 is installed.

   b. Type a rule name in *Web publishing rule name* and click *Next*
   c. Select *Allow* as the rule action and click *Next*.
   d. Select *Publish a single Web site or load balancer* as the publishing type and click *Next*.
   e. Select a connection type between the ISA Server and the published Web site and click *Next*.

      For example, select *Use non-secured connections to connect the published Web server or server farm*.

f. Type the internal name of the Web site you are publishing (for example, the machine name hosting BI platform) in *Internal site name* and click *Next*.

> **Note**
>
> If the machine hosting ISA 2006 cannot connect to the target server select *Use a computer name or IP address to connect to the published server* and type the name or IP address in the field provided.

g. In *Public Name Details* select the domain name (for example *Any domain name*) and specify any internal publishing details (for example **/***). Click *Next*.
You now need to create a new web listener to monitor for incoming Web requests.

5. Click *New* to launch the New Web Listener Definition Wizard.
   a. Type a name in *Web listener name* and click *Next*.
   b. Select a connection type between the ISA Server and the published Web site and click *Next*.
   For example, select *Do not require SSL secured connections with clients*.
   c. In *Web Listener IP Addresses* section select the following and click *Next*.
      - Internal
      - External
      - Local Host
      - All Networks

      ISA Server is now configured to publish only over HTTP.
   d. Select an *Authentication Setting* option, click *Next*, and then click *Finish*.
   The new listener is now configured for the web publishing rule.
6. Click *Next* in *User Sets*, then click *Finish.*
7. Click *Apply* to save all the settings for the web publishing rule and update the ISA 2006 configuration.
You now have to update the properties of the web publishing rule to map paths for the web applications.
8. In the navigation panel, right-click the Firewall Policy you configured and select *Properties*.
9. On the *Paths* tab, click *Add* to map routes to SAP BusinessObjects web applications.
10. On the *Public Name* tab, select *Request for the following Web sites* and click *Add*.
11. In the *Public Name* dialog box, type your ISA 2006 server name and click *OK*.
12. Click *Apply* to save all the settings for the web publishing rule and update the ISA 2006 configuration.
13. Verify the connections by accessing the following URL:

    http://<ISA Server host Name>:<web listener port number>/<External path of the application>

    For example: **http://myISAserver:80/Product/BOE/CMC**

> **Note**
>
> You may have to refresh the browser several times.

Next Steps

You need to modify the HTTP policy for the rule have just configured to ensure that you will be able to logon on to the CMC. Right-click the rule you created in the ISA Server Management utility and select *Configure HTTP*. You must now deselect *Verify Normalization* in the *URL Protection* area.

To remotely access the BI platform you need to create an access rule.

8.22 Special configuration for the BI platform in reverse proxy deployments

Some BI platform products need additional configuration to function correctly in reverse proxy deployments. This section explains how to perform the additional configuration.

8.22.1 Enabling reverse proxy for web services

This section describes the required procedures to enable reverse proxies for web services.

8.22.1.1 To enable reverse proxy on Tomcat

Context

To enable reverse proxy on the Tomcat web application server, you must modify the `server.xml` file. Required modifications include setting `proxyPort` as the reverse proxy server listen port and adding a new `proxyName`. This section explains the procedure.

Procedure

1. Stop Tomcat.
2. Open the `server.xml` for Tomcat.

   On Windows, `server.xml` is located at: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

   On Unix `server.xml` is located at `<CATALINA_HOME>/conf`. The default value of `<CATALINA_HOME>` is `<INSTALLDIR>/sap_bobj/tomcat`.
3. Locate this section in the server.xml file:

```
<!-- A "Connector" represents an endpoint by which requests are received
```

```
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml,text/plain,text/css,text/
javascript,text/json,application/javascript,application/json"/>
```

4. Uncomment the Connector element by removing `<!--` and `-->`.
5. Modify the value of `proxyPort` to be the reverse proxy server listen port.
6. Add a new `proxyName` attribute to the Connector's attribute list. The value of the `proxyName` must be the proxy server name which should be resolvable to the correct IP address by Tomcat.

   Example:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
               <!--See proxy documentation for more information about using
                 this.-->
               <Connector port="8082"
               maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
               enableLookups="false"
               acceptCount="100" debug="0"
connectionTimeout="20000"

proxyName="my_reverse_proxy_server.domain.com"
               proxyPort="ReverseProxyServerPort"
               disableUploadTimeout="true" />
```

   Where `my_reverse_proxy_server.domain.com` and `ReverseProxyServerPort` should be substituted by the correct reverse proxy server name and its listen port.
7. Save and close the `server.xml` file.
8. Restart Tomcat.
9. Ensure the reverse proxy server maps its virtual path to the correct Tomcat connector port. In the above example, the port is 8082.

   The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy SAP BusinessObjects™ Web Services deployed on Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/
dswsbobje
               ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

Next Steps

To enable web services, the proxy name and port number have to be identified for the connector.

8.22.1.2 Enabling reverse proxy for web services on web application servers other than Tomcat

Context

The following procedure requires that BI platform web applications are successfully configured against your chosen web application server. Note that the `wsresources` are case-sensitive.

Procedure

1. Stop the web application server.
2. Specify the external URL of the Web Services in the `dsws.properties` file.

   This file is located in `dswsbobje` web application. For example, if your external is URL is `http://my_reverse_proxy_server.domain.com/dswsbobje/`, update the properties in the dsws.properties file:

   - `wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine`
   - `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
   - `wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish`
   - `wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService`
   - `wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BIPlatform`
   - `wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/LiveOffice`
3. Save and close the `dsws.properties` file.
4. Restart the web application server.
5. Ensure the reverse proxy server maps its virtual path to the correct web application server connector port. The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy BI platform web services deployed on the web application server of your choice:

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<listening port> /dswsbobje

   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

   Where `<listening port>` is the listening port of your web application server.

8.22.2 Enabling the root path for session cookies for ISA 2006

This section describes how to configure specific web application servers to enable the root path for session cookies to work with ISA 2006 as the reverse proxy server.

8.22.2.1 To configure Apache Tomcat

Context

To configure the root path for session cookies to work with ISA 2006 as the reverse proxy server, add the following to the `<Connector>` element in `server.xml`:

```
emptySessionPath="true"
```

Procedure

1. Stop Tomcat
2. Open the server.xml which is located in:

   `<CATALINA_HOME>\conf`
3. Locate the following section in the server.xml file:

   ```
   <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
   <!-- See proxy documentation for more information about using this -->
   <!--
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxS
   pareThreads="75" enableLookups="false"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyPort="80" disableUploadTimeout="true" />
   -->
   ```
4. Uncomment the Connector element by removing `<!--` and `-->`.
5. To configure the root path for session cookies to work with ISA 2006 as the reverse proxy server, add the following to the `<Connector>` element in `server.xml`:

   ```
   emptySessionPath="true"
   ```
6. Modify the value of `proxyPort` to be the reverse proxy server listen port.
7. Add a new `proxyName` attribute to the Connector's attribute list. The value must be the proxy server name which should be resolvable to the correct IP address by Tomcat.

   For example:

   ```
   <!--Define a Proxied HTTP/1.1 Connector on port 8082
   -->
   <!-- See proxy documentation for more information about using
   this -->
   ```

```
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" emptySessionPath="true"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

8. Save and close the `server.xml` file.
9. Restart Tomcat.

Next Steps

Ensure the reverse proxy server maps its virtual path to the correct Tomcat connector port. In the above example, the port is 8082.

8.22.2.2 To configure Sun Java 8.2

Context

You need to modify the `sun-web.xml` for every BI platform web application.

Procedure

1. Go to `<SUN_WEBAPP_DOMAIN>`\generated\xml\j2ee-modules\webapps\BOE\WEB-INF
2. Open `sun-web.xml`
3. After the `<context-root>` container add the following:

```
        <session-config>
                <cookie-properties>
                        <property name="cookiePath" value="/" />
                </cookie-properties>
        </session-config>
   <property name="reuseSessionID" value="true"/>
```

4. Save and close `sun-web.xml`.
5. Repeat steps1-4 for every web application.

8.22.2.3 To configure Oracle Application Server 10gR3

Context

You need to modify the `global-web-application.xml` or `orion-web.xml` for every BI platform web application's deployment directory.

Procedure

1. Go to `<ORACLE_HOME>\j2ee\home\config\`
2. Open `global-web-application.xml` or `orion-web.xml`.
3. Add the following line to the `<orion-web-app>` container:

   ```
   <session-tracking cookie-path="/" />
   ```

4. Save and close the configuration file.
5. Log onto the Oracle Admin Console:
   a. Go to *OC4J:home* > *Administration* > *Server Properties*.
   b. Select *Options* under *Command Line Options*.
   c. Click *Add another Row* and type the following:

      ```
      Doracle.useSessionIDFromCookie=true
      ```

6. Restart the Oracle server.

8.22.3 Enabling reverse proxy for SAP BusinessObjects Live Office

To enable SAP BusinessObjects Live Office's View Object in Web Browser feature for reverse proxies, adjust the default viewer URL. This can be done in the Central Management Console (CMC) or through Live Office options.

> **Note**
>
> This section assumes reverse proxies for BI launch pad and BI platform web services have been successfully enabled.

8.22.3.1 To adjust the default viewer URL in the CMC

Procedure

1. Log on to the CMC.
2. On the *Applications* page, click *Central Management Console*.
3. Select *Actions* > *Processing Settings*.
4. In the *URL* field, select the correct default viewer URL, and click *Save & Close*.
   For example:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   `ReverseProxyServer` and `ReverseProxyServerPort` are the correct reverse proxy server name and its listen port.

9 Authentication

9.1 Authentication options in the BI platform

Authentication is the process of verifying the identity of a user who attempts to access the system, and rights management is the process of verifying that the user has been granted sufficient rights to perform the requested action upon the specified object.

Security plugins expand and customize the ways in which the BI platform authenticates users. Security plugins facilitate account creation and management by allowing you to map user accounts and groups from third-party systems into the platform. You can map third-party user accounts or groups to existing BI platform user accounts or groups, or you can create new Enterprise user accounts or groups that correspond to each mapped entry in the external system.

The current release supports the following authentication methods:

- Enterprise
- LDAP
- Windows AD
- SAP
- PeopleSoft

Because the BI platform is fully customizable, the authentication and processes may vary from system to system.

9.1.1 Primary authentication

Primary authentication occurs when a user first attempts to access the system. One of two things can happen during primary authentication:

- If single sign-on is not configured, the user provides their credentials, such as their user name, password and authentication type.
  These details are entered by the users on the logon screen.

  > **Note**
  >
  > By default, only the password setting to include mixed-case character(s) in passwords is checked, unless modified by the Administrator. This requires that the password contains at least one upper-case and one lower-case character. If required, the Administrator can enforce additional password settings.

- If a method of single sign-on is configured, the credentials for the users are silently propagated.
  These details are extracted using other methods such as Kerberos or SiteMinder.

The authentication type may be Enterprise, LDAP, Windows AD, SAP, PeopleSoft Enterprise depending upon which type(s) you have enabled and set up in the Authentication management area of the Central Management

Console (CMC). The user's web browser sends the information by HTTP to your web server, which routes the information to the CMS or the appropriate platform server.

The web application server passes the user's information through a server-side script. Internally, this script communicates with the SDK and, ultimately, the appropriate security plug-in to authenticate the user against the user database.

For instance, if the user is logging on to BI launch pad and specifies Enterprise authentication, the SDK ensures that the BI platform security plug-in performs the authentication. The Central Management Server (CMS) uses the security plug-in to verify the user name and password against the system database. Alternatively, if the user specifies a different authentication method, the SDK uses the corresponding security plug-in to authenticate the user.

If the security plug-in reports a successful match of credentials, the CMS grants the user an active system identity and the following actions are performed:

- The CMS creates an Enterprise session for the user. While the session is active, this session consumes one user license on the system.
- The CMS generates and encodes a logon token and sends it to the web application server.
- The web application server stores the user's information in memory in a session variable. While active, this session stores information that allows BI platform to respond to the user's requests.

  > ⓘ Note
  >
  > The session variable does not contain the user's password.

- The web application server keeps the logon token in a cookie on the client's browser. This is only used for failover purposes, such as when you have a clustered CMS or when BI launch pad is clustered for session affinity.

  > ⓘ Note
  >
  > It is possible to disable the logon token. However, if you disable the logon token, you will disable failover.

9.1.2 Security plug-ins

Security plug-ins expand and customize the ways in which the BI platform authenticates users. The BI platform currently ships with the following plugins:

- Enterprise
- LDAP
- Windows AD
- SAP
- PeopleSoft

Security plug-ins facilitate account creation and management by allowing you to map user accounts and groups from third-party systems into the BI platform. You can map third-party user accounts or groups to existing BI platform user accounts or groups, or you can create new Enterprise user accounts or groups that correspond to each mapped entry in the external system.

The security plug-ins dynamically maintain third-party user and group listings. Once you map an external group into the BI platform, all users who belong to that group can successfully log on to the BI platform. When you

make subsequent changes to the third-party group membership, you do not need to update or refresh the listing in the BI platform. For instance, if you map an LDAP group to the BI platform, and then you add a new user to the group, the security plug-in dynamically creates an alias for that new user when he or she first logs on to the BI platform with valid LDAP credentials.

Moreover, security plug-ins enable you to assign rights to users and groups in a consistent manner, because the mapped users and groups are treated as if they were Enterprise accounts. For example, you might map some user accounts or groups from Windows AD, and some from an LDAP directory server. Then, when you need to assign rights or create new, custom groups within the BI platform, you make all of your settings in the CMC.

Each security plug-in acts as an authentication provider that verifies user credentials against the appropriate user database. When users log on to the BI platform, they choose from the available authentication types that you have enabled and set up in the Authentication management area of the CMC.

> ⓘ Note
>
> The Windows AD security plugin cannot authenticate users if the BI platform server components are running on UNIX.

9.1.3 Single sign-on to the BI platform

Single sign-on to the BI platform means that once users have logged on to the operating system, they can access applications that support SSO without having to provide their credentials again. When a user logs on, a security context for that user is created. This context can be propagated to the BI platform in order to perform SSO.

The term "anonymous single sign-on" also refers to single sign-on to the BI platform, but it specifically refers to the single sign-on functionality for the Guest user account. When the Guest user account is enabled by default, anyone can log on to the BI platform as Guest, and will have access to the system.

9.1.3.1 Single sign-on support

The term single sign-on is used to describe different scenarios. At its most basic level, it refers to a situation where a user can access two or more applications or systems but provide log-on credentials only once, making it easier to interact with the system.

Single sign-on to BI launch pad can be provided by the BI platform or by different authentication tools, depending on your application server type and operating system.

These methods of single sign-on are available if you are using a Java application server on Windows:

- Windows AD with Kerberos
- Windows AD with SiteMinder

These methods of single sign-on are available if you are using IIS on Windows:

- Windows AD with Kerberos
- Windows AD with NTLM

- Windows AD with SiteMinder

These methods of single sign-on support are available on Windows or UNIX, with any supported web application server for the platform.

- LDAP with SiteMinder
- Trusted Authentication
- Windows AD with Kerberos
- LDAP through Kerberos on SUSE 11

> **Note**
>
> Windows AD with Kerberos is supported if the Java application is on UNIX. However, BI platform services need to run on a Windows server.

The following table describes the methods of single sign-on support for BI launch pad.

Authentication Mode	CMS Server	Options	Notes
Windows AD	Windows only	Windows AD with Kerberos only	Windows AD authentication to BI launch pad and CMC is available out of the box.
LDAP	Any supported platform	Supported LDAP directory servers, with SiteMinder only	LDAP authentication to the BI launch pad and CMC is available out of the box. SSO to the BI launch pad and CMC requires SiteMinder.
Enterprise	Any supported platform	Trusted Authentication	Enterprise authentication to the BI launch pad and CMC is available out of the box. SSO with enterprise authentication to the BI launch pad and CMC requires Trusted Authentication.

9.1.3.1.1 Enabling Single sign-on for CMC

To enable SSO for CMC, follow the below mentioned steps:

Context

On the client side, cache has to be cleared before the initial CMC setup. Else, the Enterprise authentication method will be cached.

On Tomcat server, perform the below mentioned steps:

Procedure

1. On a system already configured for SSO for BILP, go to `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\custom`.
2. Create a file CmcApp.properties and mention
   - sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, siteminder
   - authentication.default=secWinAD

   in that file.
3. Restart tomcat.

   SSO for CMC is enabled.

> **Note**
>
> After session timeout of the BI Launch pad or CMC, when SSO is enabled in both cases, the user is prompted to login. On refreshing the page, the user is logged back in without having to provide any password. Pinger should not be disabled during the process.

9.1.3.2 Single sign-on to the database

Once users are logged on to the BI platform, single sign-on to the database enables them to perform actions that require database access, in particular, viewing and refreshing reports without having to provide their logon credentials again. Single sign-on to the database can be combined with single sign-on to the BI platform, to provide users with even easier access to the resources they need.

9.1.3.3 End-to-end single sign-on

End-to-end single sign-on refers to a configuration where users have both single sign-on access to the BI platform at the front-end, and single sign-on access to the databases at the back-end. Thus, users need to provide their logon credentials only once, when they log on to the operating system, to have access to the BI platform and to be able to perform actions that require database access, such as viewing reports.

In the BI platform, end-to-end single sign-on is supported through Windows AD and Kerberos.

9.2 Enterprise authentication

9.2.1 Enterprise authentication overview

Enterprise authentication is the default authentication method for the BI platform. It is automatically enabled when you first install the system (it cannot be disabled). When you add and manage users and groups, the BI platform maintains the user and group information within its database.

→ Tip

Use the system default Enterprise authentication if you prefer to create distinct accounts and groups for use with the BI platform, or if you have not already set up a hierarchy of users and groups in a third-party directory server.

You do not have to configure or enable Enterprise authentication. You can however modify Enterprise authentication settings to meet your organization's particular security requirements. You can modify Enterprise authentication settings through the Central Management Console (CMC).

9.2.2 Enterprise authentication settings

Settings	Options	Description
Password Restrictions	*Enforce mixed-case password*	This option ensures that passwords contain at least one upper-case and one lower-case character in the password. ⓘ Note By default, this option is checked. If required, it can be unchecked by the administrator.
	Enforce numeral(s) in password	This option ensures that passwords contain at least one numeric character.
	Enforce special character(s) in password	This option ensures that passwords contain at least one special character.
	Must contain at least N characters where N is	This option ensures that passwords are at least N characters long.
	Must not exceed N characters where N is	This option ensures that passwords must not exceed N characters.
	Must not contain following character sequences	This option ensures that password must not contain restricted character sequences. Default value for this is as following: Password 12345678 administrator.

Settings	Options	Description
User Restrictions	*Must change password every N day(s)*	This option ensures that the passwords do not become a liability and are regularly refreshed.
	Cannot reuse the N most recent passwords(s)	This option ensures that passwords will not routinely be repeated.
	Must wait N minute(s) to change password	This option ensures that new passwords cannot be immediately changed once entered into the system.
	Must change password after N days(s) of inactivity	This option ensures that the password must change after N days(s) of inactivity.
	Must change initial password after N days(s)	This option ensures that the initial password must change after N day(s)
Logon Restrictions	*Disable account after N failed attempts to log on*	This security option specifies how many attempts a user is allowed to log on to the system before their account is disabled.
	Reset failed logon count after N minute(s)	This option specifies a time interval for resetting the logon attempt counter.
	Re-enable account after N minute(s)	This option specifies for how long an account is suspended after N failed logon attempts.
Synchronize Data Source Credentials with Log On	*Enable and update user's data source credentials at logon time*	This option enables data source credentials after the user has logged on.
Trusted Authentication	*Trusted Authentication is enabled*	Provides the settings for setting up Trusted Authentication.
OpenID Connect Authentication	*OpenID Connect Authentication is enabled*	To enable *OpenID Connect Authentication*, please check the *OpenID Connect Authentication is enabled* checkbox. When authenticating via OpenID Connect, an internal Enterprise session is created in the BI platform

9.2.3 To change Enterprise settings

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Enterprise*.
   The *Enterprise* dialog box appears.
3. Change the settings.

> → Tip
>
> To revert all the settings to the default value click *Reset*.

4. Click *Update* to save your modifications.

Results

9.2.3.1 To change general password settings

Context

> ⓘ Note
>
> Accounts not used for an extended period of time are not automatically de-activated. Administrators must manually delete inactive accounts.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Enterprise*.
   The *Enterprise* dialog box appears.
3. Select the check box for each password setting that you want to use, and provide a value if necessary.

   The following table identifies the minimum and maximum values for each of the password-related settings you can configure.

Password setting	Default	Minimum	Recommended Maximum
Must not contain following character sequences	password 12345678 administrator	1 character	25550 characters
Must contain at least N Characters	8 characters	6 characters	255 characters
Must not exceed N characters	255 characters	13 characters	255 characters
Must change password every N day(s)	30 days	2 days	100 days

Password setting	Default	Minimum	Recommended Maximum
Cannot reuse the N most recent password(s)	3 passwords	1 password	100 passwords
Must wait N minute(s) to change password	0 minutes	0 minutes	100 minutes
Must change password after N day(s) of inactivity	20 days	2 days	365 days
Must change initial password after N day(s)	7 days	2 days	15 days
Disable account after N failed attempts to log on	10 failed	1 failed	100 failed
Reset failed logon count after N minute(s)	5 minutes	1 minute	100 minutes
Re-enable account after N minute(s)	5 minutes	0 minutes	100 minutes

4. Click *Update*.

9.2.4 SAML 2.0 Authentication

9.2.4.1 To achieve single sign-on through SAML 2.0

The Business Intelligence Platform can now be integrated to any SAML enabled portals or applications, as an authentication mechanism for single sign-on experience. This means now you can login to a cloud application like Analytics Hub or SAP Analytics Cloud and access the resources in BI applications like Fiorified BI Launch Pad or Open Document during the same logon session.

You must configure your application server to achieve single sign-on through SAML 2.0.

> **Note**
>
> Set up the following prerequisites to use the SAML authentication feature to login via the email address of:
>
> - Third-party users.
>   Use the command line parameter `"-importtpemailduringsync"` to enable the import of email addresses from a third-party system:
>   1. Add the parameter `"-importtpemailduringsync"` to *CMS* > *properties* > *Command Line Parameters*.
>   2. Restart the CMS.
>   3. Do the third-party authentication update of the third-party whose user's email you want to use for login.
>
>   The supported third-party authentication types for this feature are SAP, LDAP and WinAD.

- Enterprise users.
  Refer to SAP note 2642247.

9.2.4.2 Configuring the BI Platform as SAML Service Provider

To use the BI platform as SAML service provider, you need to configure it for SAML 2.0 authentication.

Context

In this release, the steps to configure an application server as a SAML service provider has been simplified. The following steps are removed as part of this simplification:

- Copying SAML JAR files to the BI platform's install directory
- Editing the securitycontext.xml file
- Editing the web.xml file

This means that the SAML JAR files, XML tags for each web application in securitycontext.xml file, and filters in web.xml file are made available, by default. Therefore, after following the steps below, you can enable or disable SAML 2.0 authentication for each web application through the properties file of each web application.

> **Note**
>
> Use SAP Cloud Identity Provider as the default identity provider.

> **Note**
>
> You can use Tomcat application server as a SAML service provider.

Procedure

1. Follow the procedure in Configuring Trusted Authentication with Web Sessions [page 237].
2. If you are using SAP Cloud Platform Identity Provider, export all the users and then import them to the BI platform. Refer to How to import users in bulk from Central Management Console.

   To export SAP Cloud Platform users to CSV, refer to Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service.
3. Edit the properties file by changing `logon.webssoauthnetication.framework=None` to `logon.webssoauthnetication.framework=SAML`.
   - For Fiorified BI Launch pad, go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` and edit the `fioriBI.properties` file.

- For Open Document, go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` and edit the `OpenDocument.properties` file.
- For CMC, go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` and edit the `CMCApp.properties` file.

> **Note**
>
> In addition to adding `saml.enabled=true`, set the property `sso.supported.types = trustedSession` in the `CMC\FioriBI\OpenDocument` property files.

4. To update the IDP metadata in SP, first download the IDP metadata from the respective IDP service providers, then copy the metadata file to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF` and rename it to `idp-meta-downloaded.xml`.

   For details on how to download the IDP metadata, refer to Tenant SAML 2.0 Configuration.

   > **Note**
   >
   > If the BI platform is deployed on any non-Windows machine, then you need to change the path separators in the filepath to the IDP metadata under the bean **FilesystemMetadataProvider** in the `securityContext.xml` file under `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
   >
   > For example, change `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` to `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

   If you want to generate a keystore for enabling SAML 2.0, refer to Generating a Keystore for SAML 2.0 [page 238].
5. (Optional) You can use email address as a SAML assertion attribute. See the topic To use Email Address as SAML Assertion Attribute [page 240] for more information.
6. (Optional) If you are using load balancer or a reverse proxy server, then refer to 2621904 for more information.
7. Create the WAR file using the wdeploy tool.
   a. Navigate to the path `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Use the appropriate deploy command to create the war file for application-specific versions.

   - For Windows: `wdeploy.bat <App_Server_Name><Version_Name> -DAPP=BOE predeploy`
   - For UNIX: `wdeploy.sh <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

   > **Note**
   >
   > You should replace <App_Server><Version_Name> with the type of application server and its version. For example, you can use tomcat8 for Tomcat application server v8.0.
8. Once the WAR file is created, copy the WAR file and deploy it in your application server.
9. Generate and upload the service provider metadata.

   > **Note**
   >
   > You can define the property entitybase URL in the securitycontext.xml file to generate the service provider metadata with your endpoint URL. By default, the hostname and port number that you provide in the URL are considered to download the service provider metadata.

a. Go to `http(s)://host:port/BOE/saml/metadata`.

   The XML file is automatically downloaded.

b. Upload the XML file to the identity provider. If you are using Microsoft Active Directory Federation Services as your identity provider, then see Create Relying Trust Party [page 241] for more information.

> ### Note
>
> You can use the default service provider metadata file `spring_saml_metadata.xml`, located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`, instead of generating it manually. You must replace the XML tag `<replace_withip>` with the IP address or hostname of the machine based on your network, and `<replace_withport>` with the port number of an application server. Replace HTTP with HTTPS if you have enabled HTTPS in the application server.

10. If you are using SAP Cloud Identity, to create an SAML application in IDP and upload the SP `metadata.xml` in the IDP to configure the SAML SSO to BI Platform, refer to Configure a Trusted Service Provider.

> ### Note
>
> You must generate the latest service provider metadata after the keystore file is modified.

> ### → Tip
>
> To let you check if SAML integration is successful, you are redirected to the IDP once you launch the SAML configured application (BI Launch pad, Fiorified BI Launch pad, or OpenDocument).

9.2.4.2.1 Configuring Trusted Authentication with Web Sessions

You need to configure trusted authentication with web sessions as part of configuring an application server as a SAML service provider.

Context

> ### Note
>
> Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

Procedure

1. Create the `global.properties` file under the custom folder `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.
2. Enter the following as the content of the `global.properties` file:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

> **Note**
>
> You should ensure to maintain the same values for `trusted.auth.user.param` and `trusted.auth.shared.secret` parameters as updated in the *custom.jsp* file.

3. Refer Enabling Trusted Authentication [page 243] in for more information to configure trusted authentication.
4. Update the custom.jsp file with the shared secret key value for classic BI Launch Pad and Fiorified BI Launch Pad. See Editing the custom.jsp File [page 377] for more information.

> **Note**
>
> You should update the custom.jsp file if you're using Microsoft ADFS and Microsoft Azure as your identity provider.

9.2.4.2.2 Generating a Keystore for SAML 2.0

To use your own keystore file for SAML 2.0, you need to generate it.

Context

SAML exchanges use cryptography to sign and encrypt data. A sample self-signed keystore file, `sampletestKeystore.jks`, is packaged with the product and is valid till October 18, 2019. `sampletestKeystore.jks` has an alias name **Testkey** and password **Password1**.

You can now generate a self-signed keystore file using the JAVA utility keytool.

Procedure

1. Navigate to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Run the command: `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Command	Description
-alias	Enter the alias name of the certificate
-keypass	Enter the certificate's password
-keystore	Name of the keystore file
-validity	Validity of the certificate
numberofdays	Number of days for which the self-signed certificate is valid.

Answer the following questions when prompted after executing the command:

- Enter keystore password: *****
- Re-enter new password: *****
- What is your first and last name? : **MY_FIRST_AND_LAST_NAME**
- What is the name of your organizational unit? : **MY_ORGANIZATIONAL_UNIT**
- What is the name of your organization? : **MY_ORGANIZATION**
- What is the name of your city or locality? : **MY_CITY**
- What is the name of your state or province? : **MY_STATE**
- What is the two-letter country code for this unit? : **COUNTRY_CODE**

The keystore file is generated at `INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.`

3. Move the keystore file to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
4. Edit the `securityContext.xml` file located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` with the new alias name, password, and keystore file name.

   Refer to the XML code below:

   Sample Code

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

Refer to the table below to understand the arguments:

XML Tag	Description
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Locates the keystore file
`<constructor-arg type="java.lang.String" value="Password1"/>`	Password for the keystore file
`<entry key="aliasname" value="password"/>`	Alias password
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Alias of the default certificate

9.2.4.2.3 To use Email Address as SAML Assertion Attribute

You can enable email authentication on SAML for the Fiorified BI Launch pad, OpenDocument, and the Central Management Console (CMC).

Procedure

1. Depending on the application you are working on, edit the appropriate properties file by adding these two lines:

```
saml.enabled=true
saml.isUseEmailAddress=true
saml.authType=secEnterprise
```

> **Note**
>
> `saml.isUseEmailAddress` takes boolean values, and `saml.authType` corresponds to the authentication type of the user/alias details with which the login is expected to happen. The email feature can be handled individually for each application listed above. If `saml.isUseEmailAddress` is set to `false`, login happens based on the name parameter. If set to `true`, login happens based on the email parameter. `saml.authType` checks for potential duplicates and ensures that two aliases with the same authentication type can't have the same email address.

   - For the Fiorified BI Launch pad, `fioriBI.properties` under `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
   - For Opendocument, `OpenDocument.properties` under `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

- For the CMC, `CMCApp.properties` under `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

> **Note**
>
> For the CMC make sure to set the `sso.supported.types = trustedSession` property in the `CMCApp.properties` file.

2. Configure the IDP for email support. You can also refer to the SAP Cloud Platform Identity Authentication Service guide for more information if you are using SAP Cloud Identity Provider.
   a. Access the tenant's administration console URL for SAP Cloud Platform Identity Authentication service.

   > **Note**
   >
   > The URL has the form `https://<tenant ID>.accounts.ondemand.com/admin` . The tenant ID is automatically generated by the system. The first administrator created for the tenant receives an activation e-mail with a URL containing the tenant ID.

   b. Select *Applications*.
   c. Select an application.
   d. In the *Trust* tab, under the *SAML 2.0* section, click *Name ID Attribute*.
   e. Select *Email*.
   f. Click *Save*.

9.2.4.2.4 Create Relying Trust Party

You need to create a relying trust party and a claim rule in Microsoft ADFS Management tool to update the service provider metadata.

Procedure

1. Launch *Server Manager*.
2. Go to *Tools* > *AD FS Management*.
3. Expand *Trust Relationships*.
4. Right-click *Relying Trust Party* and select *Add Relying Trust Party*.
5. In the *Add Relying Trust Party* wizard, select *Start*.
6. Select *Import data about the relying party from a file* and select *Browse*.
7. Browse to the downloaded service provider metadata file and select it.
8. Select *Next*.
9. Enter the *Display Name* and select *Next*.
10. In the *Configure Multi-factor Authentication Now?* step, select *Next*.
11. Select *Permit all users to access this relying party* and select *Next*.

12. Review the information in *Ready to Add Trust* screen and select *Next*.
13. Select *Finish*.
    The *Edit Claim Rules* dialog box appears. You can create claim rules with username or email address as an attribute.

Results

You have now created a relying trust party successfully.

9.2.4.2.4.1 Creating a Claim Rule With Username as Attribute

You can create a claim rule with username as an SAML assertion attribute

Prerequisites

A relying party trust should be available.

Procedure

1. In the *Edit Claim Rules* dialog box, select *Add Rule*.
2. In the *Add Transform Claim Rule Wizard*, choose *Send LDAP Attributes as Claims* and select *Next*.
3. Enter the *Claim rule name* and select *Active Directory* as *Attribute store*.
4. Under *LDAP Attribute*, select *SAM-Account Name*.
5. Under *Outgoing Claim Type*, select *Name ID*.
6. Select *Finish*.

Results

The claim rule is created for username as an attribute.

9.2.4.2.4.2 Creating a Claim Rule With E-mail Address as Attribute

You need to create two claim rules to use email address as a SAML assertion attribute.

Procedure

1. In the *Edit Claim Rules* dialog box, select *Add Rule*.
2. In the *Add Transform Claim Rule Wizard*, choose *Send LDAP Attributes as Claims* and select *Next*.
3. Enter the *Claim rule name* and select *Active Directory* as *Attribute store*.
4. Under *LDAP Attribute*, choose *E-Mail-Addresses* and then, under *Outgoing Claim Type*, choose *E-Mail Address*.
5. In the second entry, under *LDAP Attribute*, choose *Given Name* and then, under *Outgoing Claim Type*, type *FirstName*.
6. Select *Finish*.

   You have created the first rule. Follow the steps below to create the second claim rule.
7. In the *Edit Claim Rules* dialog box, select *Add Rule*.
8. In the *Add Transform Claim Rule Wizard*, choose *Transfer an Incoming Claim* and select *Next*.
9. Enter the *Claim rule name*, choose *E-mail Address* as *Incoming claim type*, *Name ID* as *Outgoing claim type*, and *Email* as *Outgoing name format*.
10. Select *Finish*.

9.2.5 Enabling Trusted Authentication

Enterprise Trusted Authentication is used to perform single sign-on by relying on the web application server to verify the identity of a user. This method of authentication involves establishing trust between the Central Management Server (CMS) and the web application server hosting the BI platform web application. When the trust is established, the system defers the verification of the identity of a user to the web application server. Trusted Authentication can be used to support authentication methods such as SAML, x.509, and other methods, which do not have dedicated authentication plugins.

Users prefer to log on to the system once, without needing to provide passwords several times during a session. Trusted Authentication provides a Java single sign-on solution for integrating your BI platform authentication solution with third-party authentication solutions. Applications that have established trust with the Central Management Server (CMC) can use Trusted Authentication to allow users to log on without providing their passwords.

To enable Trusted Authentication, you must configure both the server and the client. To enhance the security, a new method of Trusted Authentication has been implemented in 4.3 SP04 Patch 1000+ & BI 2025. There are different behaviors depending on the installation work flow for 4.3 SP04 patch 1000 & BI 2025 and above. On **Update** to 4.3 SP04 patch 1000+ & BI 2025, Trusted Authentication will continue to work using the global shared secret if Trusted Authentication is enabled and configured before upgrade (no impact to existing work

flows). On Fresh installation of 4.3 SP04 patch 1000+ & BI 2025, Trusted Authentication can only be configured using the new method.

To learn more, see 3559381.

⚠ Caution

- In case of an update installation, it is **critically important** that you do not restart the CMS if *Trusted Authentication is Enabled* is unchecked until the new method is working fine. Otherwise, the old method is disabled permanently.
- By security design - it is no longer possible to use Trusted Authentication for the Administrator user.
- Before you are able to use Trusted Authentication, you must have either created Enterprise users, or mapped the third-party users that need to sign on to the BI platform.
- For all the supported scenarios with the new implementation of Trusted authentication, see 3559381.
- Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

Related Information

To configure the server to use Trusted Authentication with legacy method [page 245]
To configure Trusted Authentication for the web application [page 253]

9.2.5.1 Trusted Authentication for RESTful Web Services on Web Server

Context

The topic provides instructions to enable trusted authentication for RESTful web services on web server.

ⓘ Note

Trusted Authentication for the RESTful web services is unsecure.

Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

Follow the steps below to enable Trusted Authentication:

Procedure

1. Add the Web Application Server URL through the application Authorized URL Configuration.
2. Add the *Retrieving Method* and *User Name Parameter*. Refer the table below to add the Retrieving Method and User Name Parameter.

   RESTful Web Service - Trusted Authentication Configuration properties

Property	Description	Default Value
Retrieving Method	This setting is a menu that sets which query method will be used to retrieve trusted authentication logon tokens when using the RESTful web service API `/logon/trusted`. • *HTTP_HEADER* is used for GET queries with the request header accept=application/xml (or application/json). • *QUERY_STRING* is used to add a logon name to the end of a URL query using the RESTful Web Service API, for example /logon/trusted/?user=johndoe. • *COOKIE* is used when the login name is retreived from a web browser cookie. The domain, name, value and path must be stored in the cookie.	**HTTP_HEADER**
User Name Parameter	This is the label used to identify the trusted user for the purposes of retrieving a logon token.	**X-SAP-TRUSTED-USER**

3. Save the *biprws.properties file*.
4. Restart the web server.

9.2.5.2 To configure the server to use Trusted Authentication with legacy method

Prerequisites

Before you can configure Trusted Authentication, you must have created Enterprise users or mapped third-party users who need to sign on to the BI platform.

> **Note**
>
> Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Enterprise*.

   The **Enterprise** dialog box appears.
3. Select *Trusted Authentication is enabled*.
4. Create a shared secret for your users.

   > ⓘ Note
   >
   > The shared secret is used by the client and the CMS to create a trusted authentication password. This password is used to establish trust.
5. Enter a time-out value for your trusted authentication requests.

   > ⓘ Note
   >
   > The time-out value determines how long the CMS waits for the `IEnterpriseSession.logon()` call from the client application.
6. Click *Update*.

9.2.5.3 To configure the server to use Trusted Authentication with new method (Fresh Installation)

Prerequisites

- **HTTPS** must be configured on the direct web application server (eg Tomcat) that BI is accessible with, for configuration steps, see your Web Application Server documentation. SSL offloading via Load Balancers is not recommended.
- It is recommended, but not essential, that CORBA SSL is configured, see 3026364 and 2634052.

Context

The Central Management Server (CMS) now generates a secure passphrase for each web application server (WAS) and transmits it over HTTPS. To enable this communication, you must configure the URLs through which the BI platform is accessible.

Procedure

1. Navigate to *Central Management Console (CMC* > *Authentication* > *Enterprise*.
2. Check the option *Trusted Authentication is Enabled*.
3. Click *Update*.
4. Navigate to *Central Management Console (CMC* > *Applications* > *Authorized URL Configuration*.
5. Enter a system for each URL through which the BI platform is accessible. Ensure that each URL is resolvable from the CMS host.

   For each system, perform the following steps:
   - Select *Enable*.
   - Enter a unique name for the system.
   - Specify the URL in the following format:`https://<HOST>:<PORT>/BOE/CMC/TrustedAuthSetTokenServlet`

   1. The hostname and port above must be the direct Tomcat (or other supported WAS) URL, accessible via HTTPS from the operating system of any system hosting a CMS.
   2. It is only required to have one URL for each Web Application Server in an application server cluster (/BOE/CMC/TrustedAuthSetTokenServlet will work for all web applications, eg /BI, /OpenDocument).
   3. The HTTPS certificate must be valid for this hostname (via Common Name / CN or Subject Alternative Name / SAN).
6. Click *Save & Close*.
7. Repeat step 5 and 6 for each web application server (e.g. tomcat) URL in the BI environment (not loadbalancer URL).

9.2.5.4 To configure the server to use Trusted Authentication with new method (Update Installation)

Prerequisites

- **HTTPS** must be configured on the direct web application server (eg Tomcat) that BI is accessible with, for configuration steps, see your Web Application Server documentation. SSL offloading via Load Balancers is not recommended.
- It is recommended, but not essential, that CORBA SSL is configured, see 3026364 and 2634052.

Context

The Central Management Server (CMS) now generates a secure passphrase for each web application server (WAS) and transmits it over HTTPS. To enable this communication, you must configure the URLs through which the BI platform is accessible.

Procedure

1. On the Tomcat/webapp machine, Navigate to `\SAP BusinessObjects Enterprise XI 4.0\win64_x64 or /sap_bobj/enterprise_xi40/linux_x64`.
2. Rename the `TrustedPrincipal.conf` as `TrustedPrincipal.conf.old`.
3. Restart Tomcat.
4. Navigate to *Central Management Console (CMC)* > *Applications* > *Authorized URL Configuration*.
5. Enter a system for each URL through which the BI platform is accessible. Ensure that the URLs are resolvable from the CMS hosts.
6. For each System, select *Enable*, give a unique name, and enter in the URL, in the format below:

   `https://<HOST>:<PORT>/BOE/CMC/TrustedAuthSetTokenServlet`

   1. The hostname and port above must be the direct Tomcat (or other supported WAS) URL, accessible via HTTPS from the operating system of any system hosting a CMS.
   2. It is only required to have one URL for each Web Application Server in a cluster (`/BOE/CMC/TrustedAuthSetTokenServlet` will work for all web applications, eg BILP)
   3. The HTTPS certificate must be valid for this hostname (via Common Name / CN or Subject Alternative Name / SAN)

   > **Note**
   >
   > When a URL is configured and enabled, the new trusted authentication method is activated.

7. Click *Save*.
8. Repeat step 2 for each system (direct web application server URL)
9. Re-test the trusted authentication configuration.

9.2.5.5 Establishing Trust for the CMS to communicate with Tomcat (WAS)

Procedure

1. Back up the `cacerts.pem` file.

   The file is located in one of the following directories:

- **Windows**: `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\config`
- **Linux/Unix**: `/SAP BusinessObjects Enterprise XI 4.0/linux_x64/config`

Example: `cacerts.pem.org`

2. Retrieve the chain of issuer certificates in PEM format.
3. Place the exported certificate into the same directory from step 1.
4. Open a command prompt or terminal in that directory.
5. Append the chain of certificates to the cacerts .pem file. Use one of the following commands:
   - Linux: `cat chain.pem >> cacerts.pem`
   - Windows: `type chain.pem >> cacerts.pem`

9.2.5.5.1 Implementing client certificate authentication on the trusted URL

To implement client certificate authentication, first configure the server to use CORBA SSL with a CA-signed certificate. After this prerequisite is met, configure the Tomcat HTTPS connector to require client authentication.

In the `server.xml file`, duplicate the existing HTTPS connector and assign it a different port with client authentication enabled.

For example, if the existing HTTPS connector listens on port 8443, define a second connector on port 8453 as shown below:

Sample Code

```
<Connector port="8453"
           protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="200"
           maxHttpHeaderSize="65536"
           SSLEnabled="true"
           scheme="https"
           secure="true">
    <SSLHostConfig protocols="TLSv1.2"
                   certificateVerification="required"
                   caCertificateFile="C:/SSL/cacert.pem">
        <Certificate certificateKeystoreFile="file:///C:/SSL/tomcat.p12"
                     certificateKeystorePassword="Password1"
                     certificateKeystoreType="PKCS12"
                     certificateKeyPassword="Password1"
                     certificateKeyAlias="tomcat" />
    </SSLHostConfig>
</Connector>
```

If the client certificate is not trusted by the JVM running the web application server, add the issuing CA certificate to the JVM truststore.

Alternatively, on Tomcat, you can specify a dedicated truststore for client certificate authentication by using the `caCertificateFile` attribute in the `SSLHostConfig`.

The trusted URL must be configured to use this HTTPS connector.

9.2.5.6 To configure the client to use Trusted Authentication with legacy method

Context

Perform the following steps on the client machine:

Procedure

1. Create a valid configuration file.
2. Ensure the following conditions are met:
   - The file name must be `TrustedPrincipal.conf`.
   - The file must be located in the following directory:
     `businessobjects_root/win32_x86/`
   - The file must include the following entry:
     `SharedSecret=<secretPassword>`
     Replace **`<secretPassword>`** with the trusted authentication password.

9.2.6 Configuring Trusted Authentication for the Web Application

To configure Trusted Authentication for the client, you must modify global properties for the `BOE.war` file and specific properties for BI launch pad and OpenDocument applications.

Use one of the following methods to pass the user name to the client:

- `REMOTE_USER`
- `WEB_SESSION`
- `USER_PRINCIPAL`

The method you use to pass the user name must be customized in the `Trusted.auth.user.retrieval` global properties for the `BOE.war` file.

> **Note**
>
> Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

9.2.6.1 Using Trusted Authentication for SAML single sign-on

Security Assertion Markup Language (SAML) is an XML-based standard for communicating identity information. SAML provides a secure connection where identity and trust is communicated thereby enabling a single sign-on mechanism that eliminates additional logins for trusted users seeking to access the BI platform.

Enabling SAML authentication

If your application server can work as a SAML service provider, you can use Trusted Authentication to provide SAML SSO to the BI platform.

To do this, you must first configure the web application server for SAML authentication.

Also, you must use one of these methods to pass the user name to the client:

- `REMOTE_USER`
- `USER_PRINCIPAL`

The example below contains a sample web.xml configured for SAML authentication:

```
<security-constraint>
      <web-resource-collection>
        <web-resource-name>InfoView</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>j2ee-admin</role-name>
        <role-name>j2ee-guest</role-name>
        <role-name>j2ee-special</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <login-config>
      <auth-method>FORM</auth-method>
      <realm-name>InfoView</realm-name>
      <form-login-config>
        <form-login-page>/logon.jsp</form-login-page>
        <form-error-page>/logon.jsp</form-error-page>
      </form-login-config>
    </login-config>
    <security-role>
      <description>Assigned to the SAP J2EE Engine System Administrators</
description>
      <role-name>j2ee-admin</role-name>
    </security-role>
    <security-role>
      <description>Assigned to all users</description>
      <role-name>j2ee-guest</role-name>
    </security-role>
    <security-role>
      <description>Assigned to a special group of users</description>
      <role-name>j2ee-special</role-name>
    </security-role>
```

Please refer to your application server documentation for further instructions on how to accomplish this, as they will vary by application server.

Using Trusted Authentication

Once your web application server is configured to work as a SAML service provider, you can use Trusted Authentication to provide SAML SSO.

Dynamic aliasing is used to enable the SSO. When a user first accesses the logon page through SAML, they will be asked to manually log in using their existing BI platform account credentials. Once the user's credentials are verified, the system will alias the user's SAML identity to their BI platform account. Subsequent logon attempts for the user will be performed using SSO, as the system will have the user's identity alias dynamically matched to an existing account.

> **Note**
>
> Users must either be imported into the BI platform or have Enterprise accounts.

> **Note**
>
> A specific property for the BOE war file - `trusted.auth.user.namespace.enabled` - must be enabled for this mechanism to work.

9.2.6.2 Trusted Authentication properties for web applications

The following table lists Trusted Authentication settings in the default `global.properties` for the `BOE.war` file. To overwrite the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> **Note**
>
> Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

Property	Default value	Description
`sso.enabled=true`	`sso.enabled=false`	Enables and disables single sign-on (SSO) to the BI platform. Set to `true` to enable Trusted authentication.
`trusted.auth.shared.secret`	None	Session variable name used to retrieve the secret for Trusted Authentication. Only applies if using the web session to pass the shared secret.

Property	Default value	Description
`trusted.auth.user.param`	None	Specifies the variable used to retrieve the user name for Trusted Authentication.
`trusted.auth.user.retrieval`	None	Specifies the method used to retrieve the user name for Trusted Authentication: • `REMOTE_USER` • `WEB_SESSION` • `USER_PRINCIPAL` Set to blank to disable Trusted Authentication.
`trusted.auth.user.namespace.enabled`	None	Enables and disables dynamic binding of aliases to existing user accounts. If set to `true`, Trusted Authentication uses alias binding to authenticate users to the BI platform. With alias binding, your application server can work as a SAML service provider, enabling Trusted Authentication to provide SAML single sign-on to the system. If this property is blank, Trusted Authentication will use name matching when authenticating users.
`trusted.auth.url`	Your trusted auth URL	Specifies the trusted auth URL

9.2.6.3 To configure Trusted Authentication for the web application

Prerequisites

Various mechanisms populate the user name variable that is used to configure Trusted Authentication for the client hosting web applications. Configure or set up your web application server so that your user names are exposed before you use the user retrieval name methods. See http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html for further information.

Context

To configure Trusted Authentication for the client, you must access and modify properties for the `BOE.war` file, which includes general and specific properties for BI launch pad and OpenDocument web applications.

> **Note**
>
> Additional steps may be required, depending on how you plan to retrieve the user name.

Procedure

1. Access the custom folder for the `BOE.war` file on the computer hosting the web applications:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Later, you must redeploy the modified `BOE.war` file.
2. Create a new file, using Notepad or another text editing utility.
3. Enter the following Trusted Authentication properties:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=<Method for user ID retrieval>
   trusted.auth.user.param=<User Variable>
   trusted.auth.url=<trusted auth url>
   ```

   For the `trusted.auth.user.retrieval` property, select one of the following options for user name retrieval:

Option	How the user name will be retrieved
`WEB_SESSION`	The user name is retrieved from the contents of a specified session variable. You specify the web session variable to use in the `trusted.auth.user.param` property in `global.properties`.
`REMOTE_USER`	The user name is retrieved from a call to `HttpServletRequest.getRemoteUser()`.
`USER_PRINCIPAL`	The user name is retrieved from a call to `getUserPrincipal().getName()` on the `HttpServletRequest` object for the current request in a servlet or JSP.

   > **Note**
   >
   > Some web application servers require the environment variable `REMOTE_USER` set to `true` on the server. To find out whether this is required, see your web application server documentation. If it is required, confirm that the environment variable is set to `true`.

> **Note**
>
> If you are using `USER_PRINCIPAL` or `REMOTE_USER` to pass the user name, leave the `trusted.auth.user.param` blank.

4. Save the file with the name `global.properties`.
5. Restart the web application server.

Next Steps

The new properties take effect only after the modified BOE web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

9.2.6.3.1 Sample configurations

9.2.6.3.1.1 To pass the shared secret through the TrustedPrincipal.conf file

Context

User information is stored and passed through the web session, and the shared secret is passed via the `TrustedPrincipal.conf` file, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64` directory. The bundled version of Tomcat is the web application server.

Procedure

1. In the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory, create a new file, using Notepad or any other text editing utility.
2. To specify Trusted Authentication properties, enter the following values:

```
sso.enabled=true
trusted.auth.user.retrieval=<Method for user ID retrieval>
trusted.auth.user.param=<User Variable>
```

3. Save the file with the name **`global.properties`**.
4. Locate the `custom.jsp` file inside the `web` folder in the `com.businessobjects.webpath.InfoView.jar` file at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.

5. Insert the following custome java code to the `custom.jsp` file in the `com.businessobjects.webpath.InfoView.jar` file:

```
<%
//custom Java code
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> **Note**
>
> In the code snippet above, the variable <Username> should be a valid Enterprise user in the BI platform.

6. Restart the web application server.
7. Use WDeploy to redeploy the WAR file on the web application server.

   For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

Next Steps

To verify that you have properly configured Trusted Authentication, use the following URL to access BI launch pad: `http://<[cmsname]>:8080/BOE/BI/custom.jsp` where `<[cmsname]>` is the name of the machine hosting the CMS. You are prompted to enter your username and password only the first time. On successful authentication, you are automatically redirected to the BI launch pad.

9.2.6.3.1.2 To pass the shared secret through the web session variable

Context

Both the user information and the shared secret will be stored and passed via a web session variable. Open the TrustedPrincipal.conf file that have been saved earlier and note the content of the file. In this sample configuration, it is assumed the shared secret is the following:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc6577
3841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

The bundled version of Tomcat is the web application server.

Procedure

1. Access the following directory:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`

2. Create a new file using a text editor.
3. Specify the trusted authentication properties by entering the following:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

4. Save the file under the following name:

   `global.properties`

5. Access the following file:

   Classical BI Launch Pad: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`

   Fiorified BI Launch Pad: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.FioriBI\web\custom.jsp`

6. Modify the contents of the file to include the following:

```
<%
//custom Java code
request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8
211293486774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b
6a3f1345285b55a0a7");
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> ### Note
>
> In the code snippet above, the variable <Username> should be a valid Enterprise user in the BI platform.

7. Restart the web application server.
8. Use WDeploy to redeploy the WAR file on the web application server.

   For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

Next Steps

To verify that you have properly configured Trusted authentication, use the following URL to access the BI launch pad application: `http://[cmsname]:8080/BOE/BI/custom.jsp` where [cmsname] is the name of the machine hosting the CMS. You are prompted to enter your username and password only the first time. On successful authentication, you are automatically redirected to the BI launch pad.

9.2.6.3.1.3 To pass the user name through user principal

Prerequisites

The following sample configuration assumes that a user called “JohnDoe” has been created in the BI platform.

Context

User information is stored and passed through the User Principal option, and the shared secret is passed via the `TrustedPrincipal.conf` file, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` directory. The bundled version of Tomcat is the web application server.

Procedure

1. Stop the Tomcat server.
2. Open the `server.xml` file for Tomcat, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\` directory.
3. Locate the `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>`, and change it to the following value:

   ```
   Realm className=" org.apache.catalina.realm.UserDatabaseRealm".../
   ```

4. Open the `tomcat-users.xml` file, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\` directory.
5. Locate the `<tomcat-users>` tag and modify the following value:

   ```
   <user name=“JohnDoe” password=“password”
   roles=“onjavauser”/>
   ```

6. Open the `web.xml` file in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` directory.
7. Before the `</web-app>` tag, add the following values:

   ```
   <security-constraint>
       <web-resource-collection>
            <web-resource-name>OnJavaApplication</web-resource-name>
            <url-pattern>/*</url-pattern>
       </web-resource-collection>
       <auth-constraint>
            <role-name>onjavauser</role-name>
       </auth-constraint>
   </security-constraint>
   <login-config>
       <auth-method>BASIC</auth-method>
       <realm-name>OnJava Application</realm-name>
   </login-config>
   ```

   Enter a specific page for the `<url-pattern></url-pattern>` parameter. Typically, this page is not the default URL for BI launch pad or any other web application.
8. In the custom `global.properties` file, enter the following values:

   ```
   trusted.auth.user.retrieval=USER_PRINCIPAL
   trusted.auth.user.namespace.enabled=true
   ```

> **Note**
>
> Setting `trusted.auth.user.namespace.enabled=true` is optional. Add the parameter when you want to map an external user name to a different BI platform user name.

9. Restart the web application server.
10. Use WDeploy to redeploy the WAR file on the web application server.

    For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

Results

The configurations on the web application server are the same if using the Remote User method.

Next Steps

To verify that you have properly configured Trusted authentication, use the following URL to access BI launch pad: `http://<[cmsname]>:8080/BOE/BI`, where `<[cmsname]>` is the name of the machine hosting the CMS. After a few moments, a logon dialog box appears.

9.3 LDAP authentication

9.3.1 Using LDAP authentication

This section provides a general description of how LDAP authentication works with the BI platform. It then introduces the administration tools that allow you to manage and configure LDAP accounts to the platform.

When you install the BI platform, the LDAP authentication plug-in is installed automatically, but not enabled by default. To use LDAP authentication, you need to first ensure that you have your respective LDAP directory set up. For more information about LDAP, refer to your LDAP documentation.

Lightweight Directory Access Protocol (LDAP), a common, application-independent directory, enables users to share information among various applications. Based on an open standard, LDAP provides a means for accessing and updating information in a directory.

LDAP is based on the X.500 standard, which uses a directory access protocol (DAP) to communicate between a directory client and a directory server. LDAP is an alternative to DAP because it uses fewer resources and simplifies and omits some X.500 operations and features.

The directory structure within LDAP has entries arranged in a specific schema. Each entry is identified by its corresponding distinguished name (DN) or common name (CN). Other common attributes include the organizational unit name (OU), and the organization name (O). For example, a member group may be located

in a directory tree as follows: cn=BI platform Users, ou=Enterprise Users A, o=Research. Refer to your LDAP documentation for more information.

Because LDAP is application-independent, any client with the proper privileges can access its directories. LDAP offers you the ability to set up users to log on to the BI platform through LDAP authentication. It provides users with access rights to objects in the system. As long as you have an LDAP server (or servers) running, and use LDAP in your existing networked computer systems, you can use LDAP authentication (along with Enterprise, and Windows AD authentication).

If desired, the LDAP security plug-in provided with the BI platform can communicate with your LDAP server using an SSL connection established using either server authentication or mutual authentication. With server authentication, the LDAP server has a security certificate which the BI platform uses to verify that it trusts the server, while the LDAP server allows connections from anonymous clients. With mutual authentication, both the LDAP server and the BI platform have security certificates, and the LDAP server must also verify the client certificate before a connection can be established.

The LDAP security plug-in provided with the BI platform can be configured to communicate with your LDAP server via SSL, but always performs basic authentication when verifying users' credentials. Before deploying LDAP authentication in conjunction with the BI platform, ensure that you are familiar with the differences between these LDAP types. For details, see RFC2251, which is currently available at http://www.faqs.org/rfcs/rfc2251.html .

Related Information

Configuring LDAP authentication [page 261]
Mapping LDAP groups [page 272]

9.3.1.1 LDAP security plugin

The LDAP security plug-in allows you to map user accounts and groups from your LDAP directory server to the BI platform; it also enables the system to verify all logon requests that specify LDAP authentication. Users are authenticated against the LDAP directory server, and have their membership in a mapped LDAP group verified before the CMS grants them an active BI platform session. User lists and group memberships are dynamically maintained by the system. You can specify that the platform use a Secure Sockets Layer (SSL) connection to communicate to the LDAP directory server for additional security.

LDAP authentication for the BI platform is similar Windows AD authentication in that you can map groups and set up authentication, access rights, and alias creation. Also as with NT or AD authentication, you can create new Enterprise accounts for existing LDAP users, and can assign LDAP aliases to existing users if the user names match the Enterprise user names. In addition, you can do the following:

- Map users and groups from the LDAP directory service.
- Map LDAP against AD. There are a number of restrictions if you configure LDAP against AD.
- Specify multiple host names and their ports.
- Configure LDAP with SiteMinder.

Once you have mapped your LDAP users and groups, all of the BI platform client tools support LDAP authentication. You can also create your own applications that support LDAP authentication.

Related Information

Configuring SSL settings for LDAP Server or Mutual Authentication [page 265]
Mapping LDAP against Windows AD [page 275]
Configuring the LDAP plug-in for SiteMinder [page 269]

9.3.2 Configuring LDAP authentication

To simplify administration, the BI platform supports LDAP authentication for user and group accounts. Before users can use their LDAP user name and password to log on to the system, you need to map their LDAP account to the BI platform. When you map an LDAP account, you can choose to create a new account or link to an existing BI platform account.

Before setting up and enabling LDAP authentication, ensure that you have your LDAP directory set up. For more information, refer to your LDAP documentation.

Configuring LDAP authentication includes the following tasks:

- Configuring the LDAP host
- Preparing the LDAP server for SSL (if required)
- Configuring the LDAP plug-in for SiteMinder (if required)

> **Note**
>
> If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.

9.3.2.1 To configure the LDAP host

Context

It is recommended that your LDAP server be installed and running before configuring the LDAP host.

Procedure

1. Select *Authentication* from the navigation list to go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.
3. If you are setting up LDAP authentication for the first time, click *Start LDAP Configuration Wizard*.
4. Enter the name and port number of your LDAP hosts in the *Add LDAP host (hostname:port)* field (for example, "myserver:123"), click *Add*, and then click *Next*.

> → Tip
>
> Repeat this step to add more than one LDAP host of the same server type if you want to add hosts that can act as failover servers. If you want to remove a host, highlight the host name and click *Delete*.

5. Select your server type from the *LDAP Server Type* list.

> ⓘ Note
>
> If you are mapping LDAP to AD, select *Microsoft Active Directory Application Server* for your server type.

6. If you want to view or change any of the LDAP server attribute mappings or LDAP default search attributes, click *Show Attribute Mappings*.

   By default, each supported server type's server attribute mappings and search attributes are set.
7. Click *Next*.
8. In the *Base LDAP Distinguished Name* field, type the distinguished name (for example, o=SomeBase) for your LDAP server, and click *Next*.
9. In the *LDAP Server Administration Credentials* area, specify the distinguished name and password for a user account that has read access to the directory.

   Administrator credentials are not required.

   If your LDAP Server allows anonymous binding, leave this area blank. BI platform servers and clients will bind to the primary host via anonymous logon.
10. If you have configured referrals on your LDAP host, enter the authentication information in the *LDAP Referral Credentials* area and enter the number of referral hops in the *Maximum Referral Hops* field.

    You must configure the *LDAP Referral Credentials* area if all of the following criteria apply:
    - The primary host has been configured to refer to another directory server that handles queries for entries under a specified base.
    - The host being referred to has been configured to not allow anonymous binding.
    - A group from the host being referred to will be mapped to the BI platform.

> ⓘ Note
>
> Although groups can be mapped from multiple hosts, only one set of referral credentials can be set. Therefore, if you have multiple referral hosts, you must create a user account on each host that uses the same distinguished name and password.

> ⓘ Note
>
> If *Maximum Referral Hops* is set to zero, no referrals will be followed.

11. Click *Next*.
12. Choose the type of Secure Sockets Layer (SSL) authentication used:
    - *Basic (no SSL)*
    - *Server Authentication*
    - *Mutual Authentication*

Details and prerequisites for both Server and Mutual authentication are discussed in a subsequent section. To successfully set up LDAP authentication using either type of SSL, review *Configuring SSL settings for LDAP Server or Mutual Authentication* in this document before proceeding further in this procedure.

13. Click *Next*, and select a method of LDAP single sign-on authentication:
    - *Basic (no SSO)*
    - *SiteMinder*
14. Click *Next*, and select how aliases and users are mapped to BI platform accounts.
    a. In the *New Alias Options* area, select how new aliases are mapped to Enterprise accounts:
       - *Assign each added LDAP alias to an account with the same name*
         Use this option when you know users have an Enterprise account with the same name; that is, LDAP aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and LDAP account, are added as new users.
       - *Create a new account for every added LDAP alias*
         Use this option when you want to create a new account for each user.

    b. In the *Alias Update Options* area, select how to manage alias updates for the Enterprise accounts:
       - *Create new aliases when the Alias Update occurs*
         Use this option to automatically create a new alias for every LDAP user mapped to the BI platform. New LDAP accounts are added for users without BI platform accounts or for all users if you selected *Create a new account for every added LDAP alias*.
       - *Create new aliases only when the user logs on*
         Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use the BI platform. The system does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.

    c. In the *New User Options* area, specify how new users are created:
       - *New users are created as named users*
         New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

         > **Note**
         >
         > Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in.
         >
         > However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

       - *New users are created as concurrent users*
         New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the platform, a 100-user concurrent license could support 250, 500, or 700 users.

15. Perform this step if you are setting up user attribute mappings or if you plan to import email addresses from the LDAP server. In the *Attribute Binding Options* area, specify the attribute binding priority for the LDAP plugin:
    a. Click the *Import Full Name, Email Address and other attributes* box.
    The full names and descriptions used in the LDAP accounts are imported and stored with the user objects in the system.
    b. Specify an option for *Set priority of LDAP attribute binding relative to other attribute bindings*.

    > ⓘ Note
    >
    > If the option is set to 1, LDAP attributes take priority in scenarios where LDAP and other plugins (Windows AD and SAP) are enabled. If the option is set to 3, attributes from other enabled plugins will take priority.

16. Click *Finish* .

Related Information

Configuring SSL settings for LDAP Server or Mutual Authentication [page 265]
Configuring the LDAP plug-in for SiteMinder [page 269]

9.3.2.2 Managing multiple LDAP hosts

When using LDAP and the BI platform, you can add fault tolerance to your system by adding multiple LDAP hosts. The system uses the first host that you add as the primary LDAP host. Subsequent hosts are treated as failover hosts.

The primary LDAP host and all failover hosts must be configured in exactly the same way, and each LDAP host must refer to all additional hosts from which you want to map groups. For more information about LDAP hosts and referrals, see your LDAP documentation.

To add multiple LDAP Hosts, enter all hosts when you configure LDAP using the LDAP configuration wizard (see for details.) Or if you have already configured LDAP, go to the Authentication management area of the Central Management Console and click the LDAP tab. In the LDAP Server Configuration Summary area, click the name of the LDAP host to open the page that enables you to add or delete hosts.

> ⓘ Note
>
> Make sure that you add the primary host first, followed by the remaining failover hosts.

> ⓘ Note
>
> If you use failover LDAP hosts, you cannot use the highest level of SSL security (that is, you cannot select "Accept server certificate if it comes from a trusted Certificate Authority and the CN attribute of the certificate matches the DNS hostname of the server.")

Related Information

Configuring LDAP authentication [page 261]

9.3.2.3 Configuring SSL settings for LDAP Server or Mutual Authentication

This section contains detailed information on Server or Mutual SSL-based authentication for LDAP. Preliminary steps are required for setting up SSL-based authentication. This section also provides specific information for configuring SSL with LDAP Server and Mutual Authentication in the CMC. It assumes that you have configured the LDAP host and that you selected either of these for your SSL authentication choice.

For additional information or for information on configuring the LDAP host server, refer to your LDAP vendor documentation.

For Windows systems, the default SSL communication is over TLS 1.2. For Linux systems, please refer to the SAP Note 2623529.

Related Information

To configure the LDAP host [page 261]

9.3.2.3.1 To configure the LDAP Server or Mutual Authentication

Prerequisites

Resource	Take this action before starting this task
CA certificate	This action is required for both server and Mutual Authentication with SSL. 1. Obtain a Certificate Authority (CA) to generate a CA certificate. 2. Add the certificate to your LDAP Server. For information, see your LDAP vendor documentation.
Server certificate	This action is required for both server and Mutual Authentication with SSL. 1. Request and then generate a server certificate. 2. Authorize the certificate and then add it to the LDAP Server.

Resource	Take this action before starting this task

cert7.db or cert8.db, key3.db	These files are required for both server and Mutual Authentication with SSL.
	1. Download the certutil application that generates either a `cert7.db` or `cert8.db` file (depending on your requirements) from https://developer.mozilla.org/en-US/docs/NSS/tools .
	2. Copy the CA certificate to the same directory as the certutil application.
	3. Use the following command to generate the `cert7.db` or `cert8.db`, `key3.db`, and `secmod.db` files:
	`certutil -N -d .`
	4. Use the following command to add the CA certificate to the `cert7.db` or `cert8.db` file:
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	5. Store the three files in a directory on the computer that hosts the BI platform.

cacerts	This file is required for Mutual Authentication with SSL for Java applications, like BI launch pad. 1. Locate the `keytool` file in your Java `bin` directory. 2. Use the following command to create the `cacerts` file: `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` 3. Store the `cacerts` file in the same directory as the `cert7.db` or `cert8.db` and `key3.db` files.
Client certificate	1. Create separate client requests for the `cert7.db` or `cert8.db` and `.keystore` files: • To configure the LDAP plugin, use the certutil application to generate a client certificate request. • Use the following command to generate the client certificate request: `certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .` `<client_dn>` includes information such as "CN=`<client_name>`, OU=`<org unit>`, O=`<Companyname>`, L=`<city>`, ST=`<province>`, and C=`<country>`.

Resource	Take this action before starting this task

	2. Use the CA to authenticate the certificate request. Use the following command to retrieve the certificate and insert it in the `cert7.db` or `cert8.db` file:
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. To facilitate Java authentication with SSL:
	• Use the keytool utility in the Java `bin` directory to generate a client certificate request.
	• Use the following command to generate a key pair:
	`keytool -genkey -keystore .keystore`
	4. After specifying information about your client, use the following command to generate a client certificate request:
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. After the client certificate request is authenticated by the CA, use the following command to add the CA certificate to the `.keystore` file:
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. Retrieve the client certificate request from the CA, and use the following command to add it to the `.keystore` file:
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. Store the `.keystore` file in the same directory as the `cert7.db` or `cert8.db` and `cacerts` files on the computer that hosts the BI platform.

Procedure

1. Choose the level of SSL security to use.

   If you are using the LDAP configuration wizard to configure LDAP authentication for the first time, select *Mutual Authentication* from the *Type of SSL authentication* list, and click *Next*. Or, if you are reconfiguring your LDAP authentication configuration, go to the *Authentication* area of the CMC, and double-click *LDAP*. The *LDAP Server Configuration Summary* page appears. Click the *SSL Type* value, and select *Mutual Authentication* from the *Type of SSL authentication* list.

- *Always accept server certificate*
  This is the lowest security option. Before BI platform can establish an SSL connection with the LDAP host (to authenticate LDAP users and groups), it must receive a security certificate from the LDAP host. The BI platform does not verify the certificate it receives.
- *Accept server certificate if it comes from a trusted Certificate Authority*
  This is a medium security option. Before the BI platform can establish an SSL connection with the LDAP host (to authenticate LDAP users and groups), it must receive and verify a security certificate sent to it by the LDAP host. To verify the certificate, the system must find the CA that issued the certificate in its certificate database.
- *Accept server certificate if it comes from a trusted Certificate Authority, and the CN attribute of the certificate matches the DNS hostname of the server*
  This is the highest security option. Before the BI platform can establish an SSL connection with the LDAP host (to authenticate LDAP users and groups), it must receive and verify a security certificate sent to it by the LDAP host. To verify the certificate, the BI platform must find the CA that issued the certificate in its certificate database and be able to confirm that the CN attribute on the server certificate exactly matches the LDAP host name you entered in the *Add LDAP host* box in the first step of the wizard—if you entered the LDAP host name as **`ABALONE.rd.crystald.net:389`**. (Using **`CN=ABALONE:389`** in the certificate doesn't work.) .
  The host name on the server security certificate is the name of the primary LDAP host. If you select this option, you cannot use a failover LDAP host.

> **Note**
>
> Java applications ignore the first and last setting and accept the server certificate only if it comes from a trusted CA.

2. In the *SSL host* box, type the host name of each computer, and click *Add*.

   Next, you must add the host name of each computer in your BI platform deployment that uses the BI platform SDK. (This includes the computer running your Central Management Server and the computer running your web application server.)
3. Specify the SSL settings for each SSL host you added to the list:
   a. Select *default* in the SSL list.
   b. Clear the *Use default value* check boxes.
   c. Type a value in the *Path to the certificate and key database files* box and the *Password for the key database* box.
   d. If specifying settings for mutual authentication, type a value in the *Nickname for the client certificate in the certificates database* box.

> **Note**
>
> The default settings will be used (for any setting) for any host with the *Use default value* check box selected or for any computer name you do not add to the list of SSL hosts.

4. Specify the default settings for each host that isn't in the list, and click *Next*.

   To specify settings for another host, select the host name in the list on the left, and type values in the boxes on the right.

> **Note**
>
> The default settings will be used for any setting (for any host) with the *Use default value* check box selected or for any computer name you do not add to the list of SSL hosts.

5. Select *Basic (no SSO)* or *SiteMinder* as the method of LDAP single sign-on authentication.
6. Choose how new LDAP users and aliases are created.
7. Click *Finish*.

Related Information

Configuring the LDAP plug-in for SiteMinder [page 269]

9.3.2.4 To modify your LDAP configuration settings

Context

After you have configured LDAP authentication using the LDAP configuration wizard, you can change LDAP connection parameters and member groups on the *LDAP Server Configuration Summary* page.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   If LDAP authentication is configured, the *LDAP Server Configuration Summary* page appears. On this page, you can change any connection parameter areas or fields and modify options in the *Mapped LDAP Member Groups* area.
3. Delete currently mapped groups that will no longer be accessible under the new connection settings, and click *Update*.

   You can delete mapped groups by selecting the user group and then clicking the *Delete* button in the *Mapped LDAP Member Groups* section.
4. Change your connection settings, and click *Update*.
5. Change your *New Alias Options*, *Alias Update Options*, and *New User Options* if necessary, and click *Update*.
6. Map your new LDAP member groups, and click *Update*.

9.3.2.5 Configuring the LDAP plug-in for SiteMinder

This section explains how to configure the CMC to use LDAP with SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the LDAP security plug-in to create single sign-on to the BI platform.

To use SiteMinder and LDAP with the BI platform, you need to make configuration changes in two places:

- LDAP plug-in through the CMC
- `BOE.war` file properties

> **Note**
>
> Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done, regardless of what supported version of SiteMinder you are using. For more information about SiteMinder and how to install it, refer to the SiteMinder documentation.

Related Information

To configure the LDAP host [page 261]

9.3.2.5.1 To Install ETPKI Libraries

You should install the ETPKI libraries to secure the information exchanged between CA Single Sign-on Policy Server and the BI platform.

Prerequisites

Before installing ETPKI libraries, you need to download and install CA Single Sign-On SDK.

Context

The BI platform supports only CA Single Sign-On 12.x. If you have an earlier version of CA Single Sign-On, formerly known as CA Siteminder, you need to upgrade to version 12.x.

Procedure

1. Go to `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install-64` for 64-bit and `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install` for 32-bit operating systems.

   > **Note**
   >
   > If the CA Single Sign-On setup is not installed in the machine where the BI platform is installed, then copy the ETPKI libraries to the same machine.

2. Install ETPKI libraries in a Linux environment:

a. Log in with root access and execute the command `./setup install caller=sdk veryverbose`. The installation successful message appears at the end of the console or installation.
b. Execute the commands `export CAPKIHOME=/opt/CA/SharedComponents/CAPKI` and `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<BOE_INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` to set the path as the installation directory with the BI platform user.
c. Restart *Server Intelligence Agent*.

3. Install ETPKI libraries in a Windows environment:
   a. Launch command prompt with administrative privileges from the ETPKI library location.
   b. Execute the command `setup.exe install caller=sdk veryverbose`.
   c. Check the *capki_install.log* within *%temp%* for the installation success message.
   d. Restart *Server Intelligence Agent*.

Results

You have installed the ETPKI libraries successfully.

9.3.2.5.2 To configure LDAP for single sign-on with SiteMinder

Procedure

1. Open the *Please configure your SiteMinder settings* screen using one of the following methods:
   - Select SiteMinder on the *Please choose a method of LDAP single sign-on authentication* screen in the LDAP configuration wizard.
   - Select *Single Sign-On Type* on the LDAP authentication screen, which is available if you have already configured LDAP and are now adding SSO.
2. In the *Policy Server Host* box, type the name of each policy server, and then click *Add*.
3. For each Policy Server Host, specify the *Accounting*, *Authentication* and *Authorization* port numbers.
4. Enter the name of the *Agent Name* and the *Shared Secret*. Re-enter the shared secret in the *Confirm Shared Secret* box.
5. Click *Next*.
6. Proceed with configuring the LDAP options.

9.3.2.5.3 To enable LDAP and SiteMinder in the BOE.war file

Context

In addition to specifying SiteMinder settings for the LDAP security plugin, SiteMinder settings must be specified for the BOE.war properties.

Procedure

1. Go to the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory in your BI platform installation.
2. Create a new file, using Notepad or any other text editing utility.
3. Enter the following statement:

   ```
   siteminder.authentication=secLDAP
   siteminder.enabled=true
   ```

4. Close the file and save it under the **`global.properties`** name, without a file extension.
5. Create another file in the same directory.
6. Enter the following statement:

   ```
   authentication.default=secLDAP
   cms.default=[<your cms name>]:[<the CMS port number>]
   ```

   For example:

   ```
   authentication.default=secLDAP
   cms.default=mycms:6400
   ```

7. Close the file and save it under the `bilaunchpad.properties` name.

Next Steps

The new properties take effect only after the modified BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

9.3.3 Mapping LDAP groups

Once you have configured the LDAP host using the LDAP configuration wizard, you can map LDAP groups to Enterprise groups.

Once you have mapped LDAP groups, you can view the groups by clicking the LDAP option in the *Authentication* management area. If LDAP authentication is configured, the Mapped LDAP Member Groups area displays the LDAP groups that have been mapped to the BI platform.

> **Note**
>
> You can also map Windows AD groups to authenticate in the BI platform via the LDAP security plugin.

> **Note**
>
> If you have configured LDAP against AD, this procedure will map your AD groups.

9.3.3.1 To map LDAP groups using the BI platform

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   If LDAP authentication is configured, the LDAP summary page appears.
3. In the *Mapped LDAP Member Groups* area, specify your LDAP group (either by common name or distinguished name) in the *Add LDAP group (by cn or dn)* field, and click *Add*.

   To add more than one LDAP group, repeat this step. To remove a group, highlight the LDAP group and click *Delete*.
4. In the *New Alias Options* area, select an option to specify how to map LDAP aliases to Enterprise accounts:
   - *Assign each added LDAP alias to an account with the same name*
     Use this option when you know users have an existing Enterprise account with the same name (that is, LDAP aliases will be assigned to existing users—auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and LDAP account, are added as new LDAP users.
   - *Create a new account for every added LDAP alias*
     Use this option when you want to create a new account for each user.
5. In the *Alias Update Options* area, select an option to specify whether LDAP aliases are automatically created for all new users:
   - *Create new aliases when the Alias Update occurs*
     Use this option to automatically create a new alias for every LDAP user mapped to the BI platform. New LDAP accounts are added for users without BI platform accounts or for all users if you selected *Create a new account for every added LDAP alias* and clicked *Update*.
   - *Create new aliases only when the user logs on*
     Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use the BI platform. The system does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.
6. In the *New User Options* area, if your BI platform license is based on users roles, select an option to specify properties of the new Enterprise accounts that are created to map to LDAP accounts:

- *New users are created as named users*
  New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system, regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

  > **Note**
  >
  > Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in.
  >
  > However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

- *New users are created as concurrent users*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.

7. Click *Update*.

9.3.3.2 To unmap LDAP groups using the BI platform

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   If LDAP authentication is configured, the LDAP summary page will appear.
3. In the "Mapped LDAP Member Groups" area, select the LDAP group you would like to remove.
4. Click *Delete*, and then click *Update*.

   The users in this group will not be able to access the BI platform.

   > **Note**
   >
   > The only exceptions to this occur when a user has an alias to an Enterprise account. To restrict access, disable or delete the user's Enterprise account.

Next Steps

To deny LDAP Authentication for all groups, clear the "LDAP Authentication is enabled" check box and click *Update*.

9.3.3.3 Mapping LDAP against Windows AD

If you configure LDAP against Windows AD (AD), note the following restrictions:

- If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.
- Users who are only members of default groups from AD will not be able to log in successfully. Users must also be a member of another explicitly created group in AD and, in addition, this group must be mapped. An example of such a group is the "domain users" group.
- If a mapped domain local group contains a user from a different domain in the forest, the user from a different domain in the forest will not be able to log in successfully.
- Users from a universal group from a domain different than the DC specified as the LDAP host will not be able to log in successfully.
- You cannot use the LDAP plug-in to map users and groups from AD forests outside the forest where the BI platform is installed.
- You cannot map in the Domain Users group in AD.
- You cannot map a machine local group.
- If you are using the Global Catalog Domain Controller, there are additional considerations when mapping LDAP against AD:

Situation	Considerations
Multiple domains when pointing to the Global Catalog Domain Controller	You can map in: • Universal groups on a child domain, • Groups on the same domain that contains universal groups from a child domain, and • Universal groups on a cross domain. You cannot map in: • Global groups on a child domain, • Local groups on a child domain, • Groups on the same domain that contain a global group from the child domain, and • Cross-domain global groups. Generally, if the group is a universal group, it will support users from cross or child domains. Other groups will not be mapped if they contain users from cross or child domains. Within the domain you are pointing to, you can map domain local, global, and universal groups.
Mapping in universal groups	To map in universal groups, you must point to the Global Catalog Domain Controller. You should also use port number 3268 instead of the default 389.

- If you are using multiple domains but not pointing to the Global Catalog Domain Controller, then you cannot map in any type of groups from cross or child domains. You can map in all types of groups only from the specific domain you are pointing to.

9.3.3.4 Using the LDAP plugin to configure SSO to the SAP HANA database

This section provides administrators with the steps required to set up and configure single sign-on (SSO) between the BI platform running on SUSE Linux 11 and the SAP HANA database. LDAP authentication using Kerberos enables AD users to be authenticated on a BI platform running on Linux - specifically SUSE. This scenario also supports single sign-on to SAP HANA as the reporting database.

> **Note**
>
> For information on how to set up the SAP HANA database, see the *SAP HANA Database - Server Installation and Update Guide*. For information on how to set up the Data Access component for SAP HANA, see the *Data Access Guide*.

Implementation overview

The following components must be in place for Kerberos SSO to work.

Component	Requirement
Domain controller	Hosted on a machine running Active Directory setup to use Kerberos authentication.
Central Management Server	Installed and running on a machine running SUSE Linux Enterprise 11 (SUSE).
Kerberos V5 client	Installed together with the required utilities and libraries on the SUSE host. **Note** Use the latest version of the Kerberos V5 client. Add the `bin` and `lib` folders to the `PATH` and `LD_LIBRARY_PATH` environment variables.
LDAP authentication plug-in	Enabled on the SUSE host.
Kerberos login configuration file	Created on the machine hosting the web application server.

Implementation workflow

The following tasks must be performed to enable BI platform users to SSO to SAP HANA using Kerberos authentication through JDBC.

1. Setting up the AD host.
2. Creating accounts and keytab files for the SUSE host and the BI platform on the AD Host.
3. Installing Kerberos resources on the SUSE host.
4. Configuring the SUSE host for Kerberos authentication.
5. Configuring Kerberos authentication options in the LDAP authentication plug-in.
6. Creating a Kerberos login configuration file for the web application host.

9.3.3.4.1 To set up the domain controller

Prerequisites

You may need to set up a trust relationship between the SUSE host and the domain controller. If the SUSE host is in the Windows domain controller, you do not have to set up the trust relationship. However, if the BI platform deployment and the domain controller are in different domains, you may need to set up a trust relationship between the SUSE Linux machine and the domain controller. This would require the following:

1. Create a user account for the SUSE machine running the BI platform.
2. Create a host Service Principal Name (SPN).

> **Note**
>
> The SPN should be formatted according to Windows AD conventions: host/`<hostname>`@`<DNS_REALM_NAME>`. Use, in lowercase, a fully qualified domain name for /`<hostname>`. The `<DNS_REALM_NAME>` should be specified in uppercase.

3. Run the Kerberos keytab setup command `ktpass` to associate the SPN with the user account:

```
c:\> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
```

Context

The following steps must be performed on the machine hosting the domain controller.

Procedure

1. Create a user account for the service running the BI platform.
2. On the *User Accounts* page, right-click the new service account and select *Properties* > *Delegation*.
3. Select *Trust this user for delegation to any service (Kerberos only)*.
4. Run the Kerberos keytab setup command `ktpass` to create an SPN account for the new service account:

```
c:\>ktpass -princ <sianame>/<service_name>@<DNS_REALM_NAME> -mapuser
<service_name> -pass <password> -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
-out <sianame>.keytab
```

> **Note**
>
> The SPN should be formatted according to Windows AD conventions: sianame/`<service_name>`@`<DNS_REALM_NAME>`. Specify the `<service name>` in lowercase otherwise your SUSE platform may not be able to resolve it. The `<DNS_REALM_NAME>` should be specified in uppercase.

Parameter	Description
`-princ`	Specifies the principal name for Kerberos authentication.
`-out`	Specifies the name of the Kerberos `keytab` file to generate. This should match the `<sianame>` used in `-princ`.
`-mapuser`	Specifies the name of the user account to which the is SPN mapped to. The Server Intelligence Agent runs on this account.
`-pass`	Specifies the password used by the service account.
`-ptype`	Specifies the principal type: `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Specifies the encryption type to use with the service account: `-crypto RC4-HMAC-NT`

Results

You have generated the required keytab files for the trust relationship between the SUSE machine and the domain controller.

Next Steps

You must transfer the keytab file(s) to the SUSE machine and store them in the `/etc` directory.

9.3.3.4.2 To set up the SUSE Linux Enterprise 11 machine

Prerequisites

The following resources are required for setting up Kerberos on the SUSE Linux machine running the BI platform:

- Keytab files created on the domain controller. The keytab file created for the BI platform service is mandatory. The keytab for the SUSE host is recommended specifically for scenarios where the BI platform host and the domain controller are in different domains.
- The latest Kerberos V5 library (including the Kerberos client) must be installed on the SUSE host. You must add the location of the binaries to the `PATH` and `LD_LIBRARY_PATH` environment variables. To verify that the Kerberos client is properly installed and configured, ensure that the following utilities and libraries exist on the SUSE host:
  - `kinit`
  - `ktutil`
  - `kdestroy`
  - `klist`
  - `/lib64/libgssapi_krb5.so.2.2`
  - `/lib64/libkrb5.so.3.3`
  - `/lib/libkrb5support.so.0.1`
  - `/lib64/libk5crypto.so.3`
  - `/lib64/libcom_err.so.2`

> → Tip
>
> Run `rpm -qa | grep krb` to check the version of these libraries. For information on the latest Kerberos client, libraries, and Unix host configuration see http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5 .

Context

After all the required resources are available on the SUSE host, follow the instructions below to set up Kerberos authentication.

> ⓘ Note
>
> To perform these steps you must have root privileges.

Procedure

1. To merge the keytab files, run the following command:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Edit the `/etc/kerb5.conf` file to refer to the domain controller (on the Windows platform) as the Kerberos Domain Controller (KDC).

   Use to the example below:

```
[domain_realm]
 .name.mycompany.corp = DOMAINNAME.COM
  name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
        forwardable = true
           default_realm = DOMAINNAME.COM
           default_tkt_enctypes = rc4-hmac
           default_tgs_enctypes = rc4-hmac

[realms]
        DOMAINNAME.COM = {
             kdc = machinename.domainname.com
            }
```

   > ⓘ Note
   >
   > The `krb5.conf` file contains Kerberos configuration information, including the locations of KDCs and servers for the Kerberos realms of interest, Kerberos applications, and mappings of hostnames onto Kerberos realms. Normally the `krb5.conf` file is installed in the `/etc` directory.

3. Add the domain controller to `/etc/hosts` so that the SUSE host can locate the KDC.
4. Run the `kinit` program from the `/usr/local/bin` directory to verify that Kerberos has been set up properly. Verify that an AD account user account can log into the SUSE machine.

   > → Tip
   >
   > The KDC should issue a Ticket Granting Ticket (TGT) which can be viewed in the cache. Use the `klist` program to view the TGT.

Example

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>
> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached
>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

Next Steps

You should also use `kinit` to test the SPNs.

9.3.3.4.3 To configure Kerberos authentication options for LDAP

Prerequisites

Before configuring Kerberos authentication for LDAP, you must first enable and configure the BI platform LDAP authentication plugin to connect to the AD directory. To use LDAP authentication, you need to first ensure that you have set up your respective LDAP directory.

> **Note**
>
> When running the *LDAP Configuration Wizard* you must specify *Microsoft Active Directory Application Server* and provide the requested configuration details.

Context

After LDAP authentication is enabled and connected to your Microsoft Active Directory Application Server, the *Enable Kerberos Authentication* area appears on the LDAP Server Configuration Summary page. Use this area to configure Kerberos authentication, which is required for single sign-on to the SAP HANA database from a BI platform deployment on SUSE.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   The *LDAP Server Configuration Summary* page appears, where you can modify any of the connection parameters or fields.
3. To configure Kerberos authentication, perform the following steps in the *Enable Kerberos Authentication* area:
   a. Click *Enable Kerberos Authentication*.
   b. Click *Cache Security Context (required for SSO to database)*.

   > ⓘ Note
   >
   > Enabling the cache security context is specifically required for single sign-on to SAP HANA.

   c. Specify the Service Principal Name (SPN) for the BI platform account in *Service Principal Name*.

   The format for specifying the SPN is `<sianame/service>`@`<DNS_REALM_NAME>` where

`<sianame>`	Name of the Server Intelligence Agent
`<service>`	Name of the service account used to run the BI platform
DNS_REALM_NAME	The domain name of the domain controller in uppercase

   > → Tip
   >
   > When specifying the SPN, remember that `<sianame/service>` is case sensitive.

   d. Specify the domain for the domain controller in *Default Kerberos Realm*.
   e. Specify `userPrincipalName` in *User Principal Name*.

   This value is used by the LDAP authentication application to provide user ID values that are required by Kerberos. The value specified should match the name provided when creating the keytab files.
4. Click *Update* to submit and save your changes.

Results

You have configured Kerberos authentication options to refer to user accounts in the AD directory.

Next Steps

You need to create a Kerberos login configuration file - `bscLogin.conf` - to enable Kerberos logon and single sign-on.

Related Information

Configuring LDAP authentication [page 261]

9.3.3.4.4 To create a Kerberos login configuration file

Context

To enable Kerberos logon and single sign-on, you need to add a login configuration file on the machine hosting the BI platform web application server.

Procedure

1. Create a file called `bscLogin.conf` and store it in the `/etc` directory.

   > **Note**
   >
   > You can store this file in a different location. However, if you do, you will need to specify its location in your Java options. It is recommended that the `bscLogin.conf` and the Kerberos keytab files reside under the same directory. In a distributed deployment, you must add a `bscLogin.conf` file for every machine hosting a web application server.

2. Add the following code to your login `bscLogin.conf` configuration file:

   ```
   com.businessobjects.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required;
   };
   com.businessobjects.security.jgss.accept {
   com.sun.security.auth.module.Krb5LoginModule required
   storeKey=true
   useKeyTab=true
   keyTab="/etc/krb5.keytab"
   principal="<principal name>";
   };
   ```

   > **Note**
   >
   > The following section is specifically required for single sign-on:
   >
   > ```
   > com.businessobjects.security.jgss.accept {
   > com.sun.security.auth.module.Krb5LoginModule required
   > storeKey=true
   > useKeyTab=true
   > keyTab="/etc/krb5.keytab"
   > principal="<principal name>";
   > };
   > ```

3. Save and close the file.

9.3.3.5 Troubleshooting new LDAP accounts

- If you create a new LDAP user account, and the account does not belong to a group account that is mapped to the BI platform, either map the group, or add the new LDAP user account to a group that is already mapped to the system.
- If you create a new LDAP user account, and the account belongs to a group account that is mapped to the BI platform, refresh the user list.

Related Information

Configuring LDAP authentication [page 261]
Mapping LDAP groups [page 272]

9.4 Windows AD authentication

9.4.1 Using Windows AD authentication

9.4.1.1 Windows AD support requirements and initial setup

This section guides you through the process of configuring Windows Active Directory (AD) authentication to work on the BI platform. All the required end-to-end workflows you need to perform are presented together with validation tests and prerequisite checks.

> ⓘ Note
>
> For additional information for configuring Windows AD authentication, refer to SAP Knowledge Base KBA 1631734 available at https://service.sap.com/sap/support/notes/1631734.

Support requirements

To facilitate AD authentication on the BI platform, you should remember the following support requirements.

- The CMS must always be installed on a supported Windows platform.
- Certain BI platform applications may only use particular authentication methods. For example, applications such as BI launch pad and Central Management Console only support Kerberos.

Recommended AD set up workflow

To initially set up manual AD authentication with the BI platform, use the following workflow:

1. Set up the Domain Controller.
2. Configure AD authentication in the CMC.
3. Configure the AD user account on the Server Intelligence Agent (SIA).
4. Configure your web application server for AD authentication with Kerberos.

> **Note**
>
> Use this workflow whether or not you require single sign-on (SSO). The workflow described in the following sections will first enable you to manually (using an AD username and password) log into the BI platform. Once you have successfully configured manual AD authentication, a detailed section is provided to guide you through the process of setting up SSO for AD authentication.

9.4.2 Preparing the Domain Controller

9.4.2.1 Setting up a service account for AD authentication with Kerberos

To configure the BI platform to work with Windows AD (Kerberos) authentication, you require a service account. You can either create a new domain account or use an existing domain account. The service account will be used to run the BI platform servers. After setting up the account, you will need to set up an SPN for the account. This SPN is used to import AD user groups into the BI platform.

> **Note**
>
> To use AD with SSO, you will need to later revisit the service account set up to grant the account appropriate rights, and configure it for constrained delegation.

9.4.2.1.1 To set up the service account on a Windows 2008 domain

Context

You need to set up a new service account to successfully enable Windows AD authentication using the Kerberos protocol. This service account will be used primarily to allow users in a given AD group to log on to BI launch pad. The following task is performed on the AD domain controller machine.

Procedure

1. Create a new service account with a password on the primary domain controller.
2. Use the `setspn -s` command to add the service principal names (SPN) to the service account you created in Step 1. Specify service principal names (SPNs) for the service account, as well as the server, fully qualified domain server and IP address for the machine on which BI launch pad is deployed.
   For example:

   ```
   setspn –s BICMS/service_account_name.domain.com serviceaccountname
   setspn -s HTTP/<servername> <servicename>
   setspn -s HTTP/<servername.domain.com> <servicename>
   setspn -s HTTP/<ip address of server> <servicename>
   ```

   `BICMS` is the name of the machine on which the SIA is running, `<servername>` is the name of the server on which BI launch pad is deployed and `<servernamedomain>` is its fully qualified domain name.
3. Run `setspn -l <servicename>` to verify that the service principal names were added to the service account.
   The output for the command should include all the registered SPNs as shown below:

   ```
   Registered ServicePrincipalNames for
   CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
   HTTP/<ip address of server>
   HTTP/<servername>.@example.com
   HTTP/<servername>
   <servername>/<servicename>@example.com
   ```

   A sample output is provided below:

   ```
   C:\Users\Admin>setspn -L bossosvcacct
   Registered ServicePrincipalNames for
   CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
           BICMS/bossosvcacct@example.com
           HTTP/Tomcat HTTP/Tomcat@example.com
           HTTP/Load_Balancer.@example.com
   ```

Next Steps

Once created, the service account needs to be granted rights and added to the server's Local Administrators group. The SPN will be used to import AD groups in the next section.

9.4.3 Configuring AD Authentication in the CMC

9.4.3.1 Windows AD Security plug-in

The Windows AD Security plug-in enables you to map user accounts and groups from your AD 2008 user database to the BI platform. It also enables the system to verify all logon requests that specify AD Authentication. Users are authenticated against the AD user database, and have their membership in a

mapped AD group verified before the Central Management Server (CMS) grants them an active session. You can use the plug-in to configure updates for the imported AD groups.

The Windows AD security plug-in enables you to configure the following:

- Windows AD authentication with Kerberos
- Windows AD authentication with NTLM
- Windows AD authentication with SiteMinder for single sign-on

The AD security plug-in is compatible with AD 2008 domains running in either native mode or mixed mode.

Once you have mapped your AD users and groups, they will be able to access BI platform client tools using the *Windows AD* authentication option.

- Windows AD authentication works if the CMS is run on Windows. For SSO to a database to work, the reporting servers must also run on Windows. Otherwise all other servers and services can run on all platforms supported by the BI platform.

  > **Note**
  >
  > The configuration has been done and tested with SUSE linux Enterprise 11 only.

- The Windows AD plug-in for the BI platform supports domains within multiple forests.

9.4.3.2 To map Windows AD users and groups

Prerequisites

Before you can import AD user groups into the BI platform, you must have completed the following prerequisite actions:

- Created a service account on the domain controller for the BI platform. The account will be used to run BI platform servers.

  > **Note**
  >
  > To enable AD authentication with Vintela single sign-on (SSO), you must provide an SPN that is configured for this purpose. The steps provided below are for configuring manual AD authentication to the BI platform. Once you have configured manual AD authentication, refer to the *Single Sign-On Setup* section in this chapter for details on how to add SSO to your AD authentication configuration.

- Verified that the SPN containing the name of the machine on which the SIA is running has been added to the service account.

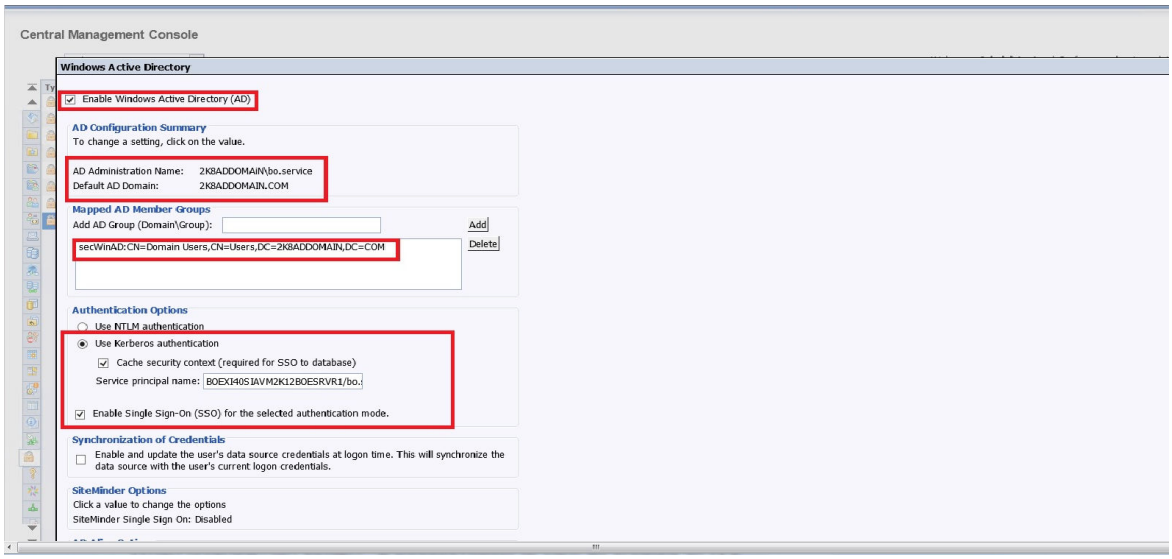
Context

Steps 1 to 11 below are mandatory to import AD groups into the BI platform.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Select the *Enable Windows Active Directory (AD)* check box.
4. In the *AD Configuration Summary* area, click the link beside *AD Administration Name*.

   > **Note**
   >
   > Before the Windows AD plug-in is configured, this link appears as quotation marks. After the configuration is saved, the link is populated with AD Administration names.



5. Enter the name and password of an enabled domain user account.

   Administration credentials can use either of the following formats:

   - NT name (`DomainName\UserName`)
   - UPN (`user@DNS_domain_name`)

   The BI platform uses this account to query information from AD. The platform does not modify, add, or delete content from AD. Because only reads information, only the appropriate rights are required.

   > **Note**
   >
   > AD authentication will break if the account used to read the AD directory becomes invalid (for example, if the account's password is changed or expires or if the account is disabled).

6. Enter the AD domain in the *Default AD Domain* box.

   The domain must be specified as the FULL DOMAIN NAME in ALL CAPS or a child domain name from where most users will be logging onto the BI platform. This should match the default domain specified in the Kerberos configuration files that are used to configure the application server. You can map groups from the default domain without specifying the domain name prefix. If you enter a default AD domain name, users from the default domain do not have to specify the AD domain name when logging onto the BI platform using AD authentication.

7. In the *Mapped AD Member Groups* area, enter the AD domain\group in the *Add AD Group (Domain\Group)* box, using one of the following formats to map groups:

   - Security Account Manager account name (SAM), also referred to as NT name (`DomainName\GroupName`)
   - DN (`cn=GroupName, ......, dc=DomainName, dc=com`)

   > **Note**
   >
   > If you want to map a local group, use only the NT name format: `\\<ServerName>\<GroupName>`. AD does not support local users; local users who belong to a mapped local group will not be mapped to the BI platform. Therefore, they cannot access the system.

   > **→ Tip**
   >
   > When manually logging onto BI launch pad, users from other domains must append the domain name, in uppercase letters, after their user name. For example `CHILD.PARENTDOMAIN.COM` is the domain in
   >
   > ```
   > user@CHILD.PARENTDOMAIN.COM
   > ```

8. Click *Add*.

   The group is added to the list under *Mapped AD Member Groups*.

9. In the *Mapped AD Member Groups* area, enter the desired AD domain\group in the *Search AD Group (Domain\Group)* field.

   This searches for the desired group from the list. You can also choose *Show* to view the complete list of AD groups in a separate dialog box.

10. Under *Authentication Options*, select *Use Kerberos authentication*.
11. In the *Service principal name* box, enter the SPN mapped to the service account you created to run BI platform servers.

> **Note**
>
> You must specify the SPN for the service account that runs the SIA. For example: `BICMS/bossosvcacct.domain.com`.

12. Click *Update*.

> **Caution**
>
> Do not proceed if users and/or groups are not mapping in properly! To resolve specific AD group mapping issues refer to SAP note 1631734.

> **Note**
>
> If you have successfully mapped AD group accounts and do not want to configure AD authentication options or AD group updates, skip steps 12 to 19. You can configure these optional settings after you have successfully set up manual AD Kerberos authentication.

13. If your configuration requires SSO to a database, select *Cache security context*.

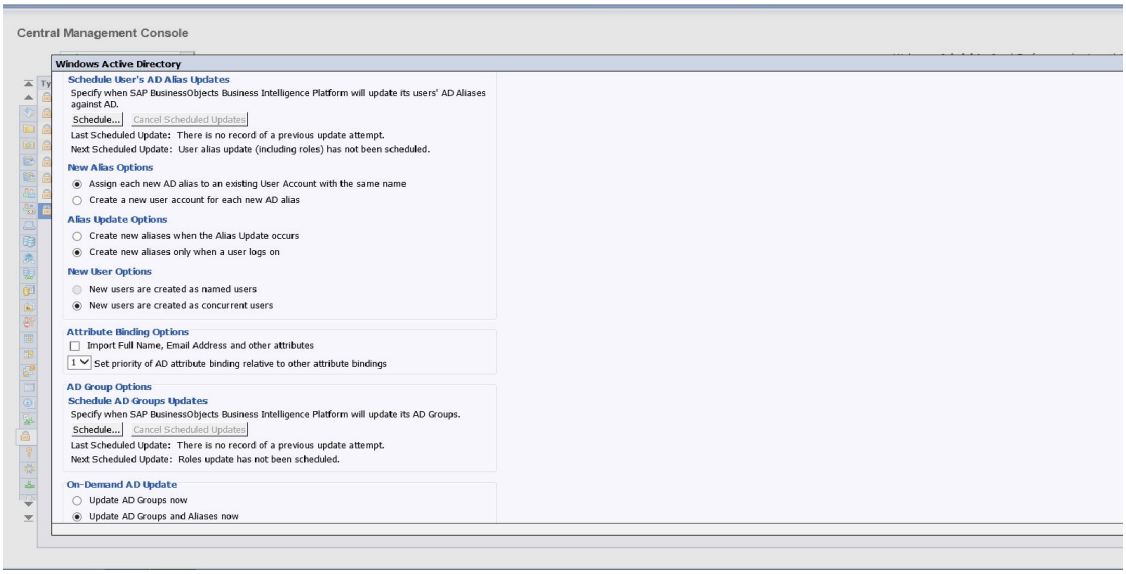
> **Note**
>
> If this is your initial AD authentication configuration, it is recommended that you first successfully set up manual AD authentication before you consider the extra configuration required for SSO.

14. Select *Enable single sign-on for selected authentication mode* if you require SSO for your AD authentication configuration.
15. In the *Synchronization of Credentials* area, select an option to enable and update the AD user's data source logon credentials .

    This option synchronizes the data source with the user's current logon credentials, thereby enabling scheduled reports to run when the user is not logged on to the BI platform and Kerberos SSO is not available.
16. In the *AD Alias Options* area, specify how new aliases are added to and updated in the BI platform.
    a. In the *New Alias Options* area, select an option for mapping new aliases to Enterprise accounts:
       - *Assign each new AD alias to an existing User Account with the same name*
         Select this option when you know users have an existing Enterprise account with the same name; that is, AD aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and AD account, are added as new users.
       - *Create a new user account for each new AD alias*
         Select this option when you want to create a new account for each user.

    b. In the *Alias Update Options* area, select an option for managing alias updates for the Enterprise accounts:
       - *Create new aliases when the Alias Update occurs*
         Select this option to automatically create a new alias for each AD user mapped to the BI platform. New AD accounts are added for users without BI platform accounts, or for all users if you selected *Create a new user account for each new AD alias* and clicked *Update*.
       - *Create new aliases only when the user logs on*
         Select this option when the AD directory you are mapping contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and Enterprise

accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.



c. In the *New User Options* area, select an option for creating new users:

- *New users are created as named users*
  New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the BI platform based on a user name and password. This provides named users with access to the system, regardless of how many people are connected. You must have a named user license available for each user account created using this option.

  > **Note**
  >
  > Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in.
  >
  > However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

- *New users are created as concurrent users*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.

17. To configure how to schedule AD alias updates, click *Schedule*.
    a. In the *Schedule* dialog box, select a recurrence from the *Run object* list.
    b. Set other schedule options and parameters as required.
    c. Click *Schedule*.
    When the alias update occurs, the group information is also updated.
18. In the *Attribute Binding Options* area, specify the attribute binding priority for the AD plugin:

a. Select the *Import Full Name, Email Address and other attributes* check box.
   The full names and descriptions used in AD accounts are imported and stored with user objects in BI platform.
b. Specify an option for *Set priority of AD attribute binding relative to other attributes binding*.
   If the option is set to 1, AD attributes take priority when AD and other plugins (LDAP and SAP) are enabled. If the option is set to 3, attributes from other enabled plugins take priority. The bindings must be set to different values. Setting multiple authentication plugins to the same binding value leads to unexpected results.

19. In the *AD Group Options* area, configure AD group updates:
    a. Click *Schedule*.
       The *Schedule* dialog box appears.
    b. Select a recurrence from the *Run object* list.
    c. Set other schedule options and parameters as required.
    d. Click *Schedule*.

    The system schedules the update and runs it according to the schedule you specified. The next scheduled update for the AD group accounts is displayed under the *AD Group Options*.
20. In the *On-Demand AD Update* area, select one of the following options:
    - *Update AD Groups now*
      Select this option if you want to start updating all scheduled AD groups when you click *Update*. The next scheduled AD group update is listed under *AD Group Options*.
    - *Update AD Groups and Aliases now*
      Select this option if you want to start updating all scheduled AD groups and user aliases when you click *Update*. The next scheduled updates are listed under *AD Group Options* and *AD Alias Options*.
    - *Do not update AD Groups and Aliases now*
      No AD groups or user aliases will be updated when you click *Update*.
21. Click *Update*, and click *OK*.

Next Steps

To verify that you have actually imported AD user accounts, go to *CMC* > *User and Groups* > *Group Hierarchy* and select the AD group you have mapped to view users in that group. The current and nested users in the AD group will be displayed.

Related Information

To create a Kerberos configuration file [page 297]

9.4.3.3 Scheduling updates for Windows AD groups

The BI platform enables administrators to schedule updates for AD groups and user aliases. This feature is available for AD authentication with either Kerberos or NTLM. The CMC also enables you to view the time and date when the last update was performed.

> **Note**
>
> For AD authentication to work on the BI platform, you must configure how updates are scheduled for your AD groups and aliases.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can specify what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will be run on the dates specified in a calendar that has previously been created.

Scheduling AD group updates

The BI platform relies on AD for user and group information. To minimize the volume of queries sent to AD, the AD plugin caches information about groups and how they relate to each other and their user membership. The update does not run when no specific schedule is defined.

You must use the CMC to configure the recurrence of the group update refresh. This should be scheduled to reflect how frequently your group membership information is modified.

Scheduling AD user alias updates

User objects can be aliased to an AD account, allowing users to use their AD credentials to log on to BI platform. Updates to AD accounts are propagated to the BI platform by the AD plug-in. Accounts created, deleted, or disabled in AD will be correspondingly created, deleted, or disabled in the BI platform.

If you do not schedule AD alias updates, updates will occur only when:

- A user logs on.
- An administrator selects the *Update AD Groups and Aliases now* option from the *On Demand AD Update* area of the CMC.

> **Note**
>
> No AD passwords are stored in the user alias.

9.4.4 Configuring the BI platform service to run the SIA

9.4.4.1 Running the SIA under the BI platform service account

To support AD Kerberos authentication for the BI platform, you must grant the service account the right to act as part of the operating system. This must be done on each machine running a Server Intelligence Agent (SIA) with the Central Management Server (CMS).

To enable the service account to run/start the SIA, you must configure specific operating system settings described in this section.

> **Note**
>
> If you will require single sign-on to the database, the SIA must include the following servers:
>
> - Crystal Reports Processing Server
> - Report Application Server
> - Web Intelligence Processing Server

9.4.4.2 To configure the SIA to run under the service account

Prerequisites

Before configuring the SIA account to run under the BI platform service account you must complete the following prerequisite actions:

- A service account has been created on the domain controller for the BI platform.
- You have verified that the required service principal names (SPN) have been added to the service account.
- You have successfully mapped AD user groups into the BI platform.

If you want to give specific rights to user, then perform the following steps:

1. Click *Start > Control Panel > Administrative Tools > Local Security Policy*.
2. Expand *Local Policies*, then click *User Rights Assignment*.
3. Double-click *Act as part of the operating system*.
4. Click *Add*, and enter the name of the service account you created, then click *OK*.

Context

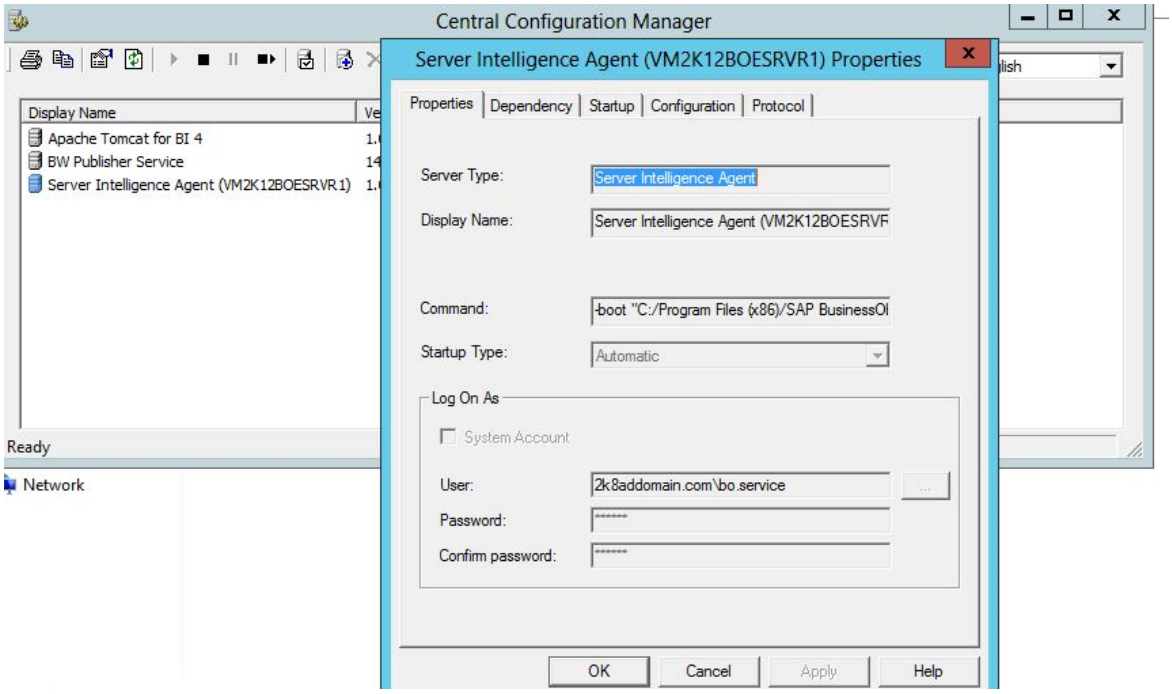
Perform this task for any Server Intelligence Agent (SIA) that is running services used by the service account.

Procedure

1. To start the CCM, choose *Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *Central Configuration Manager*.
   The CCM home page opens.
2. In the CCM, right-click the Server Intelligence Agent (SIA) and select *Stop*.

   > **Note**
   >
   > When you stop the SIA, all services managed by the SIA are stopped.

3. Right-click the SIA and select *Properties*.



4. Clear the *System Account* check box.
5. Type the service account credentials (`<DOMAINNAME>\<service name>`) and click *OK*.

   The service account must be granted the following rights on the machine running the SIA:

   - The account must specifically have the “Act as part of operating system” right.
   - The account must specifically have the “Logon as a service” right.
   - Full control rights to the folder where BI platform is installed.
   - Full control rights to “ HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects” in the system registry.
6. Repeat the above steps on each machine running a BI platform server.

   > **Note**
   >
   > It is important that the Effective Right ends up being checked after *Act as part of the operating system* is selected. Typically, you will need to restart the server for this to occur. If, after restarting the server, this option is still not on, your Local Policy settings are being overridden by your Domain Policy settings.
7. Restart the SIA.
8. If necessary, repeat steps 1 to 5 for each SIA running a service that must be configured.

Next Steps

You should now be able to login into the CCM using AD credentials.

9.4.4.3 To test AD credentials on the CCM

Prerequisites

To perform this task, you need to have successfully mapped an AD user group into the BI platform.

Procedure

1. Open the CCM and click the *Manage Servers* icon.
2. Ensure that the right information is displayed in the *System* field.
3. Select *Windows AD* from the authentication options list.
   A login dialog box opens.
4. Log on using an existing AD account from the AD group you mapped into the BI platform.

   > **Note**
   >
   > If you are using an AD account that does not reside in the default domain, login as `domain\username`.

Results

You should not receive any error messages. You must be able to log in via the CCM using a mapped AD account before moving to the next section.

> → Tip
>
> If you get an error message, go to *CMC* > *Authentication* > *Windows AD*. Under *Authentication Options*, change *Use Kerberos authentication* to *Use NTLM authentication* and click *Update*. Repeat steps 1-4 above. If this works, there is an issue with your Kerberos configuration.

9.4.5 Configuring the web application server for AD Authentication

9.4.5.1 Preparing the application server for Windows AD authentication (Kerberos)

The process of configuring Kerberos for a web application server varies slightly depending on the specific application server. However, the general process of configuring Kerberos involves these steps:

- Creating the Kerberos `(krb5.ini)` configuration file.
- Creating the JAAS login `bscLogin.conf` configuration file.

  > ⓘ Note
  >
  > This step is not required for the SAP NetWeaver 7.3 Java application server. However you will need to add the LoginModule to your SAP NetWeaver server.

- Modifying the Java options for your application server.
- Overwriting the `BOE.war` file properties for Windows AD authentication.
- Restarting your Java application server.

This section contains the details for configuring Kerberos for use with the Tomcat application server.

9.4.5.1.1 Creating Kerberos configuration files

9.4.5.1.1.1 To create a Kerberos configuration file

Prerequisites

Before proceeding, ensure you have performed the following prerequisite tasks:

- A service account has been created on the domain controller for the BI platform.

- You have verified that the service principal names (SPNs) have been added to the service account.
- You have successfully mapped AD user groups into the BI platform.
- You have tested AD credentials on the CCM.

Context

Follow these steps to create the Kerberos configuration file if you're using Tomcat as the web application server for your BI platform deployment.

Procedure

1. Create the file `krb5.ini`, if it does not exist, and store it under `C:\Windows` for Windows.

   > **Note**
   >
   > If the application server is installed on Unix, you should use the following directory:
   >
   > Linux: `/etc/krb5.conf`

   > **Note**
   >
   > You can store this file in a different location. However, you will need to specify its location in your java options. For more information on `krb5.ini` go to http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view .

2. Add the following required information in the Kerberos configuration file:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

> **Note**
>
> The key parameters are explained in the table below.

`DOMAIN.COM`	The DNS name of your domain which must be entered in uppercase in FQDN format.
`kdc`	The Host name of the Domain Controller.
`[capath]`	Defines the trust between domains that are in another AD forest. In the example above `DOMAIN2.COM` is a domain in an external forest and has direct two way transitive trust to `DOMAIN.COM`.
`default_realm`	In a multiple domain configuration, under `[libdefaults]` the `default_realm` value may be any of the source domains. The best practice is to use the domain with the greatest number of users that will be authenticating with their AD accounts. If no UPN suffix is supplied at log on, it defaults to the value of `default_realm`. This value should be consistent with the *default domain* setting in the CMC. All domains must be specified in uppercase as shown in the example above.

9.4.5.1.2 Creating a JAAS login configuration file

9.4.5.1.2.1 To create a Tomcat or WebLogic JAAS login configuration file

Context

The `bscLogin.conf` file is used to load the java login module and is required for AD Kerberos authentication on Java web application servers.

The default location for the files is: `C:\Windows`.

Procedure

1. Create a file called `bscLogin.conf` if it does not exist, and store it in `C:\Windows`.

> **Note**
>
> You can store this file in a different location. However, if you do, you will need to specify its location in your java options.

2. Add the following code to your JAAS `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Save and close the file.

9.4.5.1.2.2 To create an Oracle JAAS login configuration file

Procedure

1. Locate the `jazn-data.xml` file.

> **Note**
>
> The default location for this file is `C:\OraHome_1\j2ee\home\config`. If you installed Oracle Application Server in a different location, find the file specific to your installation.

2. Add the following content to the file between the `<jazn-loginconfig>` tags:

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Save and close the `jazn-data.xml` file.

9.4.5.1.3 Modifying the application server Java settings to load configuration files

9.4.5.1.3.1 To modify the Java options for Kerberos on Tomcat

Procedure

1. From the *Start* menu, select *Programs >Tomcat > Tomcat Configuration*.
2. Click the *Java* tab.
3. Add the following options:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

Replace XXXX with the location where you stored the `bscLogin.conf` file.

4. Close the Tomcat configuration file.
5. Restart Tomcat.

9.4.5.1.4 To verify that Java can receive a Kerberos ticket

Prerequisites

Before testing if Java has received the Kerberos ticket, you must complete the following prerequisite actions:

- Create the `bscLogin.conf` file for your application server.
- Create the `krb5.ini` file.

Procedure

1. Go to the command prompt and navigate to the `jdk\bin` directory in your BI platform installation.

   By default this is located in:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.
2. Run `kinit <username>`.
3. Press `Enter`.
4. Type the password.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\jdk\bin>kinit sfredell
Password for sfredell@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

   If the `krb5.ini` file was configured properly and the Java login module has been loaded, you should see the following message:

   `New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator`

Results

Do not continue with the AD setup until you have successfully received a Kerberos ticket.

If you cannot receive a ticket, consider the following options:

- Consult the troubleshooting section at the end of this chapter.
- For issues concerning the KDC, the Kerberos configuration files, and user credentials not available in the Kerberos database, refer to SAP Knowledge Base articles KBA 1476374 and KBA 1245178.

9.4.5.1.5 To configure BI launch pad for manual AD login

Prerequisites

Before configuring your BI platform applications for manual AD login, the following prerequisite actions must be completed:

- You have created a service account on the domain controller for the BI platform.
- You have verified that the HTTP service principal names (SPN) have been added to the service account.
- You have successfully mapped AD user groups into the BI platform.
- You have tested AD credentials on the CCM.
- You have created, configured, and tested the required configuration files for your web application server.
- Your application server's Java settings have been modified to load the configuration files.

Context

To enable the Windows AD authentication option for both BI launch pad, perform the following steps:

Procedure

1. Access the custom folder for the BOE web application on the machine hosting the web application server:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Make your changes in the `config\custom` and not the `config\default` directory. Otherwise your changes will be overwritten when future patches will be applied to your deployment.

   You will have to later redeploy the modified BOE web application.
2. Create a new file.

   > **Note**
   >
   > Use Notepad or any other text-editing utility.
3. Save the file as `BIlaunchpad.properties`.
4. Type the following:

   ```
   authentication.visible=true
   authentication.default=secWinAD
   ```
5. Save and close the file.
6. Restart your web application server.

Results

You should now be able to manually log into BI launch pad, access either application, and select Windows AD from the list of authentication options.

> **Note**
>
> Do not continue with your Windows AD setup until you can manually log into BI launch pad with an existing AD account.

Next Steps

The new properties will take effect only after the BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy BOE on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

> **Note**
>
> If your deployment uses a firewall, remember to open all the required ports; otherwise, the web applications will not be able to connect to the BI platform servers.

9.4.6 Single Sign-On Setup

9.4.6.1 SSO to the BI platform with AD authentication

Options for SSO using Windows AD

There are three supported methods for setting up single sign-on (SSO) for Windows AD authentication with the BI platform:

- Vintela - This option can only be used with Kerberos.
- SiteMinder - This option can only be used with Kerberos.

SSO to the database

SSO to the database enables logged-on users to perform actions that require database access, in particular, viewing, and refreshing reports, without having to provide their logon credentials again. While constrained delegation is optional for AD authentication and Vintela SSO, it is required for deployment scenarios that involve single sign-on to the system database.

End-to-end SSO

In the BI platform, end-to-end SSO is supported through Windows AD and Kerberos. In this scenario, users have both single sign-on access to the BI platform at the front-end, and SSO access to the databases at the back-end. Thus, users need to provide their logon credentials only once, when they log on to the operating system, to have access to the BI platform and to be able to perform actions that require database access, such as viewing reports.

Manual versus SSO AD authentication configuration

Once you have successfully configured your deployment to enable AD accounts to manually log into BI launch pad, you need to revisit the AD authentication setup to enable specific SSO requirements. Requirements will vary depending on your choice of SSO method.

9.4.6.2 Using Vintela SSO

9.4.6.2.1 Checklist for Vintela SSO setup

To set up the BI platform to work with Vintela SSO, you need to complete the following tasks:

1. Specifically configure your service account for Vintela SSO.
2. Configure constrained delegation (optional).
3. Configure the Windows AD SSO authentication options in the CMC.
4. Configure the general and BI launch pad-specific properties for Vintela SSO.
5. If you are using Tomcat as the web application server for your deployment, you need to increase the header size limit.
6. Configure the internet browsers for Vintela.

9.4.6.2.2 To set up the service account for Vintela SSO

Prerequisites

The `Ktpass` command-line tool configures the server principal name for the host or service in Active Directory and generates a Kerberos "keytab" file containing the shared secret key of the service account. This tool is usually found on domain controllers or it can be downloaded from the Microsoft support site: http://support.microsoft.com/kb/892777 .

Context

You need a service account specifically configured to allow users in a given Windows AD group to automatically authenticate to BI launch pad with their AD credentials. You can reconfigure the service account created for AD Kerberos authentication on the domain controller.

When a client attempts log into BI launch pad, a request to the Kerberos ticket-generating server is initiated. To facilitate this request, the service account created for the BI platform must have an SPN that matches the URL of the application server. Perform the following steps on the machine hosting the domain controller.

Procedure

1. Run the Kerberos keytab setup command `ktpass` to create and place a `keytab` file.

   Specify the `ktpass` parameters listed in the following table:

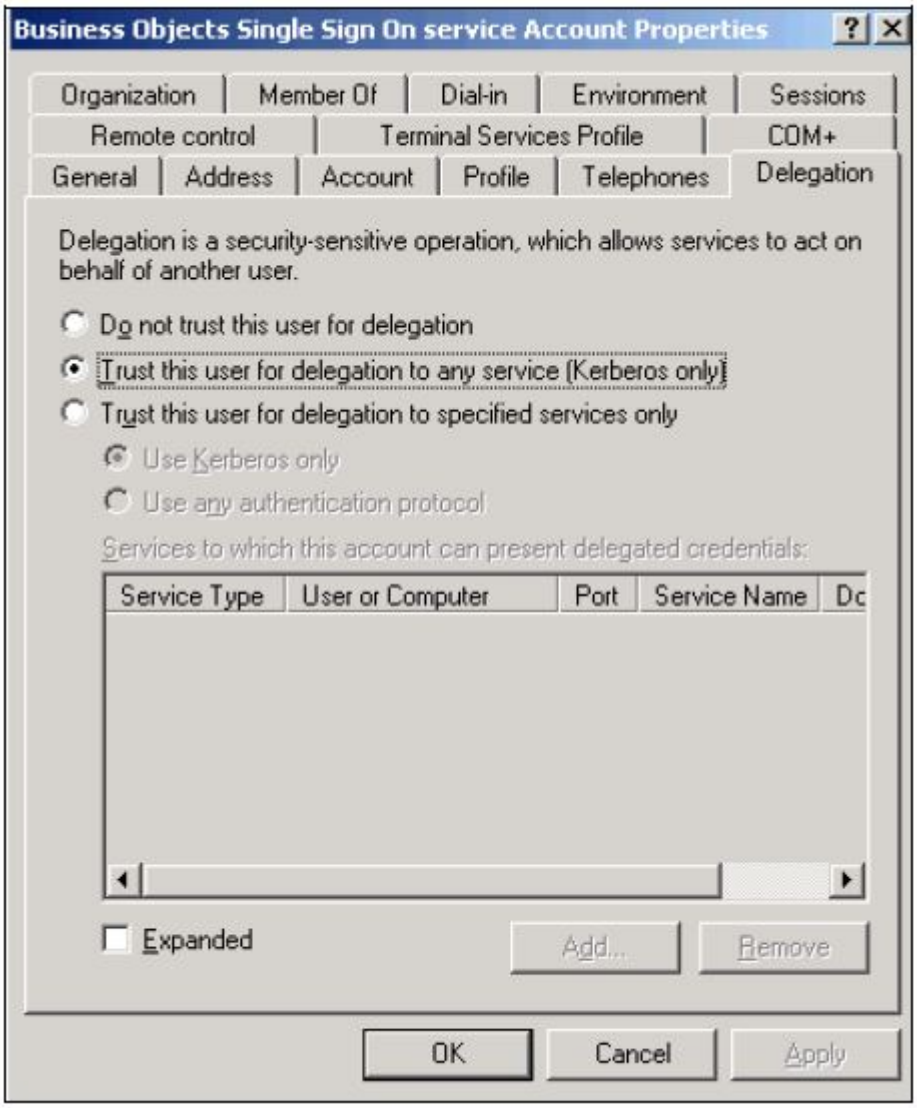
Parameter	Description
`-out`	Specifies the name of the Kerberos `keytab` file to generate.
`-princ`	Specifies the principal name used for the service account, in SPN format:`< MYSIAMYSERVER>/ <sbo.service.domain.com>@<DOMAIN>.COM`, where `<MYSIAMYSERVER>` is the name of the Service Intelligence Agent as specified in the Central Configuration Manager (CCM). **Note** The name of your service account is case-sensitive. The SPN includes the name of the host computer on which the service instance is running. **→ Tip** The SPN must be unique in the forest in which it is registered. To check, use the Windows support tool `Ldp.exe` to search for the SPN.
`-pass`	Specifies the password used by the service account.
`-ptype`	Specifies the principal type: `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Specifies the encryption type to use with the service account: `-crypto RC4-HMAC-NT`

   For example:

```
ktpass -out <keytab_filename>.keytab -princ <MYSIAMYSERVER>/
sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

   The output from the `ktpass` command should confirm the target domain controller and that a Kerberos `keytab` file containing the shared secret was created. The command also maps the principal name to the (local) service account.

2. Right-click the service account, select *Properties* > *Delegation*.
3. Click *Trust this user for delegation to any service (Kerberos only)*.



4. Click *OK* to save your settings.

Results

The service account now has all the required service principal names for Vintela SSO and you have generated a keytab file with the encrypted password for the service account.

> **Note**
>
> For end-to-end single sign on or single sign on to databases using keytab file scenarios:
>
> In cases of failures resolved by changing KVNO in the keytab, it is likely that the KVNO attribute on the service account is higher than the KVNO used in the keytab creation (during ktpass). For information on how to get the correct KV no, refer http://service.sap.com/sap/support/notes/1853668

9.4.6.2.2.1 To configure constrained delegation for Vintela SSO

Context

Constrained delegation is optional for setting up Vintela SSO. It is, however, mandatory for deployments that require SSO to the system database.

Procedure

1. On the AD domain controller machine, open the Active Directory *Users and Computers* snap-in.
2. Right-click the service account you created in the previous section, and click *Properties* > *Delegation*.
3. Select *Trust this user for delegation to the specified services only*.
4. Select *Use Kerberos only*.
5. Click *Add* > *Users or Computers*.
6. Type the service account name and click *OK*.
   A list of services is displayed.
7. Select the following services and then click *OK*.
   - The HTTP service
   - The service used to run the Service Intelligence Agent (SIA) on the machine hosting the BI platform.

   The services are added to the list of services that can be delegated for the service account.

Next Steps

You will need to modify the web application properties to account for this modification.

9.4.6.2.3 To configure SSO settings in the CMC

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Ensure the *Enable Windows Active Directory (AD)* check box is selected.
4. Under *Authentication Options*, ensure the *Use Kerberos authentication* option is selected.
5. If your configuration requires SSO to the database, select *Cache security context*.
6. Select *Enable single sign-on for selected authentication mode*.
7. Click *Update*.

9.4.6.2.4 To enable Vintela single sign-on for BI launch pad and OpenDocument

Context

This procedure is used for either BI launch pad or OpenDocument. To enable SSO to the BI platform web applications, you need to specify Vintela and SSO-specific properties in the `BOE.war` file. For SSO setup purposes, it is recommended that you concentrate on enabling SSO to BI launch pad for AD accounts before handling other applications.

Procedure

1. Access the custom folder for the BOE web application on the machine hosting the web application server:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Make your changes in the `config\custom` directory and not the `config\default` directory. Otherwise your changes will be overwritten when future patches will be applied to your deployment.

   You will have to later redeploy the modified BOE web application.
2. Create a new file using a text editor.
3. Enter the following:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
```

```
idm.logger.props=error-log.properties
```

> **Note**
>
> The `idm.realm` and `idm.princ` parameters require valid values. The `idm.realm` should be the same value you set when you configured the `default_realm` in your `krb5.ini` file. The value must be in upper case. The `idm.princ` parameter is the SPN used for the service account created for Vintela SSO.

> **Note**
>
> Forward slashes are required when specifying the keytab file location.

Skip the following step if you do not want to use constrained delegation for Windows AD authentication and Vintela SSO.

4. To use constrained delegation, add:

```
idm.allowS4U=true
```

5. Close the file and save it with a `global.properties` name.

> **Note**
>
> Make sure the file name is not saved under any extensions such as `.txt`.

6. Create another file in the same directory. Save the file as `OpenDocument.properties` or `BIlaunchpad.properties` depending on your requirements.
7. Type the following:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

For example:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Save and close the file.
9. Restart your web application server.

Next Steps

The new properties will take effect only after the BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy BOE on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

> **Note**
>
> If your deployment is using a firewall, remember to open all the required ports otherwise the web applications will not be able to connect to the BI platform servers.

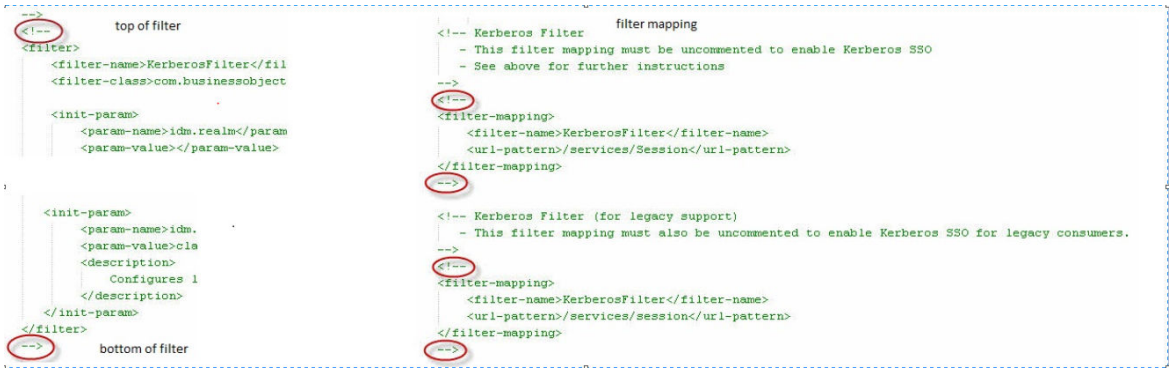
9.4.6.2.5 To enable Vintela single sign-on for Web Services

Context

Some client tools will require authentication through web services. Follow these steps to enable single sign-on (SSO) for web services. For more information, see related SAP note at: http://service.sap.com/sap/support/notes/1646920

Procedure

1. Back up this file: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml` and then open it for editing.
2. Uncomment the Kerberos Proxy Filter and Kerberos Filter sections to enable Kerberos SSO for Windows Active Directory (secWinAD) authentication.



The following options must be specified (the rest are optional):

- `idm.realm` (the same as the default_realm specified in the Krb5.ini file).
- `idm.princ` (the same as specified for idm.princ in the global.properties file located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
- `idm.keytab` (the same as specified for idm.keytab in the global.properties file located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

> **Note**
>
> If you are using the hardcoded password set in Tomcat's Java Options, do not make any changes to the keytab lines in the `web.xml` file.

3. If SSL is not in use with the Java application server, then set the idm.allowUnsecured parameter to **`true`**.

   For more information about Tomcat SSL, see the Knowledge Base Article ID:1484802.
4. Back up this file: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties` and open it for editing.
5. Set kerberos.sso to **`true`** and save the file.

6. Use WDeploy to redeploy the WAR file on the web application server.

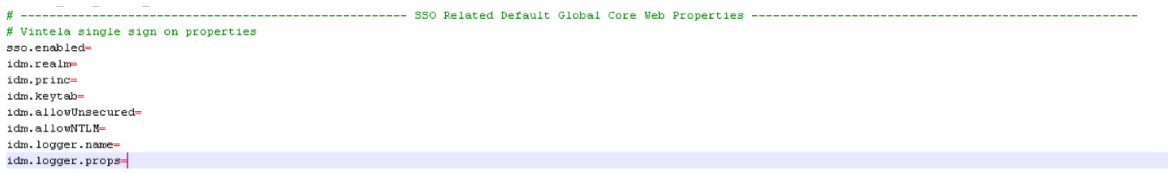
   For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

7. Restart Tomcat.

9.4.6.2.6 To enable Vintela single sign-on for RESTful Web Services

Some client tools require authentication through RESTful web services. Follow these steps to enable single sign-on (SSO) for web services.

1. Copy the file `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\biprws.properties` to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties`, and then open it to edit.
2. To enable Kerberos SSO for Windows Active Directory (secWinAD) authentication, set `sso.enabled` to `true`. See the screenshot below:

   Specify the following mandatory options:

   - `idm.realm` (the same as the default_realm specified in the Krb5.ini file).
   - `idm.princ` (the same as specified for idm.princ in the global.properties file located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - `idm.keytab` (the same as specified for idm.keytab in the global.properties file located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - `idm.allowUnsecured` parameter must be set to `true` if SSL is not in use with the Java application server. For more information about Tomcat SSL, see the *Knowledge Base Article ID:1484802*

3. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
4. Restart Tomcat.
5. To test your settings, on the client machine, open any browser and launch the URL: http://<WebAppServer>:<portnumber>/biprws/v1/logon/adsso.
   The REST token must appear as a response to the API.

9.4.6.2.7 To increase the header size limit for Tomcat

Context

Active Directory creates a Kerberos token which is used in the authentication process. This token is stored in the HTTP header. Your Java application server will have a default HTTP header size. To avoid failures, ensure that it has a minimum default size of 16384 bytes. (Some deployments may require a larger size. For more information, see Microsoft's sizing guidelines on their support site (http://support.microsoft.com/kb/327825).)

Procedure

1. On the server with Tomcat installed, open the `server.xml` file.

   On Windows, this file is located at `<TomcatINSTALLDIR>/conf`

   - If you are using the version of Tomcat installed with the BI platform on Windows, and you did not modify the default
     installation location, replace `<TomcatINSTALLDIR>` with `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\`
   - If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path.
2. Find the corresponding `<Connector ...>` tag for the port number you have configured.

   If you are using the default port of 8080, find the `<Connector ...>` tag with port="8080" in it.

   For example:

   ```
   <Connector URIEncoding="UTF-8" acceptCount="100"
   connectionTimeout="20000" debug="0"
   disableUploadTimeout="true" enableLookups="false"
   maxSpareThreads="75" maxThreads="150"
   minSpareThreads="25" port="8080" redirectPort="8443"
   />
   ```
3. Add the following value within the `<Connector ...>` tag:

   `maxHttpHeaderSize="16384"`

   For example:

   ```
   <Connector URIEncoding="UTF-8" acceptCount="100"
   connectionTimeout="20000" debug="0"
   disableUploadTimeout="true" enableLookups="false"
   maxSpareThreads="75" maxThreads="150"
   maxHttpHeaderSize="16384" minSpareThreads="25" port="8080"
   redirectPort="8443" />
   ```
4. Save and close the `server.xml` file.
5. Restart Tomcat.

Next Steps

> **Note**
>
> For other Java application servers, consult your Java application server's documentation.

9.4.6.2.8 Configuring Internet browsers

To support Vintela SSO for AD Kerberos authentication, you must configure BI platform clients. This involves configuring the web browser on the client machines.

9.4.6.2.8.1 To configure Internet Explorer on the client machines

Procedure

1. On the client machine, open an IE browser.
2. Enable integrated Windows authentication.
   a. On the *Tools* menu, click *Internet Options*.
   b. Click the *Advanced* tab.
   c. Scroll to *Security*, select *Enable Integrated Windows Authentication*, and then click *Apply*.
3. Add the Java Application machine or the URL to the trusted sites. You can enter the full domain name of the site.
   a. On the *Tools* menu, click *Internet Options*.
   b. Click the *Security* tab.
   c. Click *Sites* and then click *Advanced.*
   d. Select or enter the site and click *Add.*
   e. Click *OK* until the Internet Options dialog box closes.
4. Close and reopen the Internet Explorer browser window for these changes to take effect.
5. Repeat all of these steps on each BI platform client machine.

9.4.6.2.8.2 To configure Firefox on the client machines

Procedure

1. *Modify network.negotiate-auth.delegation-uris*
   a. On the client machine, open a Firefox browser.

b. Type **about:config** in the URL address field.
A list of configurable properties appears.
c. Double-click *network.negotiate-auth.delegation-uris* to edit the property.
d. Enter the URL that you will use to access BI launch pad.

For example if your BI launch pad URL is **http://<machine.domain.com>:8080/BOE/BI**, then you need to enter **http://<machine.domain.com>**.

> ⓘ Note
>
> To add more than one URL, separate them with a comma. For example: **http://<machine.domain.com>,<machine2.domain.com>**.

e. Click *OK*.

2. *Modify network.negotiate-auth.trusted-uris*
a. On the client machine, open a Firefox browser.
b. Type **about:config** in the URL address field.
A list of configurable properties appears.
c. Double-click *network.negotiate-auth.trusted-uris* to edit the property.
d. Enter the URL that you will use to access BI launch pad. .
For example if your BI launch pad URL is **http://<machine.domain.com>:8080/BOE/BI**, then you will need to enter **http://<machine.domain.com>**

> ⓘ Note
>
> To add more than one URL, separate them with a comma. For example: **http://<machine.domain.com>,<machine2.domain.com>**.

e. Click *OK*.

3. Close and reopen the Firefox browser window for these changes to take effect.
4. Repeat all of these steps on each BI platform client machine.

9.4.6.2.9 Testing Vintela SSO for AD Kerberos authentication

You should test your SSO setup from a client workstation. Make sure that the client is on the same domain as your BI platform deployment, and that you are logged into the workstation as a mapped AD user. This user account must be able to manually log into BI launch pad.

To test SSO, open a browser and enter the URL for BI launch pad. If SSO is properly configured, you should not be prompted for your logon credentials.

> → Tip
>
> It is recommended that you test various AD user scenarios in your deployment. For example, if your environment will have users from multiple operating systems, you should test SSO for users from each operating system. You should also test SSO against all the possible browsers supported in your organization. If your environment will have users from multiple forests or domains, you should test SSO for a user account from each domain or forest.

9.4.6.2.10 Configuring Kerberos and single sign-on to the database for application servers

Single sign-on to the database is supported for deployments that meet all these requirements:

- The deployment of the BI platform is on a web application server.
- The web application server has been configured for Vintela SSO for AD authentication.
- The database to which SSO is required is a supported version of SQL Server or Oracle.
- The groups or users that need access to the database must have been granted permissions within SQL Server or Oracle. .

The final step is to modify the `krb5.ini` file to support SSO to the database for web applications.

9.4.6.2.10.1 To enable single sign-on to the database for Java application servers

Procedure

1. Open the `krb5.ini` file that is being used for your deployment of the BI platform.
   The default location for this file is the WIN directory on your web application server.

   > **Note**
   >
   > If you cannot find the file in the WIN directory, check this Java argument for the location of the file:
   >
   > ```
   > -Djava.security.auth.login.config
   > ```
   >
   > This variable is specified when AD with Kerberos is configured on your web application server.

2. Go to the `[libdefaults]` section of the file.
3. Enter this string prior to the start of the `[realms]` section of the file:

   ```
   forwardable=true
   ```

4. Save and close the file.
5. Restart your web application server.

Next Steps

Single sign-on to the database will not be enabled until you check the *Cache security context (required for SSO to database)* box in the Windows AD authentication page in the CMC.

9.4.6.3 Using SiteMinder

9.4.6.3.1 Using Windows AD with SiteMinder

This section explains how to use AD and SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the AD security plug-in to create single sign-on to the BI platform. You can use SiteMinder with Kerberos.

Ensure your SiteMinder identity management resources are installed and configured before configuring Windows AD authentication to work with SiteMinder. For more information about SiteMinder and how to install it, refer to your SiteMinder documentation.

There are two tasks you must complete to enable AD single sign-on with SiteMinder:

- Configure the AD plug-in for single sign-on with SiteMinder
- Configure SiteMinder properties for the BOE web application

> **Note**
>
> Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done regardless of which supported version of SiteMinder you are using. For more information about SiteMinder configuration, refer to your SiteMinder documentation.

9.4.6.3.1.1 To enable SiteMinder properties for BI launch pad

Context

In addition to specifying SiteMinder settings for the Windows AD security plugin, SiteMinder settings must be specified for the BOE war properties.

Procedure

1. Locate the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory in your BI platform installation.
2. Create a new file in the directory, using Notepad or another text-editing utility.
3. In the new file, enter the following values:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Save the file with the name `global.properties`.

> **Note**
>
> Make sure the file name is not saved with an extension, such as `.txt`.

5. Create another file in the same directory.
6. In the new file, enter the following values:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

   For example:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Save the file with the name `BIlaunchpad.properties`, and close the file.

Next Steps

The new properties take effect after BOE.war is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

9.4.6.3.1.2 To configure SiteMinder settings in the CMC

Prerequisites

Before configuring the CMC for SiteMinder, you must complete the following prerequisite actions:

- You have successfully mapped AD user groups into the BI platform.
- You have tested AD credentials on the CCM.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Select the *Enable Windows Active Directory (AD)* check box.
4. Under Authentication Options, select *Use NTLM authentication* or *Use Kerberos authentication*.

   To configure the BI platform for Kerberos and AD authentication using Kerberos, you must have a service account. You can either create a new domain account or use an existing domain account. The service account will be used to run BI platform servers.

   > → Tip
   >
   > When manually logging on to BI launch pad, users from other domains must append the domain name, in uppercase letters, after their user name. For example, in `user@CHILD.PARENTDOMAIN.COM`, “CHILD.PARENTDOMAIN.COM” is the domain.

5. If you selected *Use Kerberos authentication*:
   a. If you want to configure single sign-on to a database, select *Cache security context*.
   b. Delete any information in the *Service principal name* box.
6. If you want to configure single sign-on, select *Enable Single Sign On for selected authentication mode*.

   You must also configure BOE web application general properties and BI launch pad properties to enable single sign-on.
7. In the *Synchronization of Credentials* area, select an option to enable and update the AD user's data source credentials at logon.

   This option synchronizes the data source with the user's current logon credentials.
8. In the *SiteMinder Options* area, configure SiteMinder as your single sign-on option for AD authentication using Kerberos:
   a. Click *Disabled.*

      The *Windows Active Directory* page appears.

      If you have not configured the Windows AD plug-in, a warning appears, asking if you want to continue. Click *OK*.
   b. Click *Use SiteMinder Single Sign On*.
   c. In the *Policy Server Host* box, type the name of each policy server, and click *Add*.
   d. For each policy server host, enter a port number in the *Accounting*, *Authentication*, and *Authorization* boxes.
   e. In the *Agent Name* box, enter the agent name.
   f. In the *Shared Secret* boxes, enter the shared secret.

      Ensure that the SiteMinder Administrator has enabled support for 4.x Agents, regardless of which supported version of SiteMinder you use. For information about SiteMinder and how to install it, see the SiteMinder documentation.
   g. Click *Update* to save and return to the main AD authentication page.
9. In the *AD Alias Options* area, specify how new aliases are added to and updated in the BI platform.
   a. In the *New Alias Options* area, select an option for mapping new aliases to Enterprise accounts:
      - *Assign each new AD alias to an existing User Account with the same name*
        Select this option when you know users have an existing Enterprise account with the same name; that is, AD aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and AD account, are added as new users.
      - *Create a new user account for each new AD alias*
        Select this option when you want to create a new account for each user.
   b. In the *Alias Update Options* area, select an option for managing alias updates for the Enterprise accounts:
      - *Create new aliases when the Alias Update occurs*
        Select this option to automatically create a new alias for each AD user mapped to the BI platform. New AD accounts are added for users without BI platform accounts, or for all users if you selected *Create a new user account for each new AD alias* and clicked *Update*.
      - *Create new aliases only when the user logs on*
        Select this option when the AD directory you are mapping contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.

c. In the *New User Options* area, select an option for creating new users:

- *New users are created as named users*
  New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on a user name and password. This provides named users with access to the system, regardless of how many people are connected. You must have a named user license available for each user account created using this option.

  > **Note**
  >
  > Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in.
  >
  > However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

- *New users are created as concurrent users*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.

10. To configure how to schedule AD alias updates, click *Schedule*.
    a. In the *Schedule* dialog box, select a recurrence from the *Run object* list.
    b. Set other schedule options and parameters as required.
    c. Click *Schedule*.
    When the alias update occurs, the group information is also updated.
11. In the *Attribute Binding Options* area, specify the attribute binding priority for the AD plugin:
    a. Select the *Import Full Name, Email Address and other attributes* check box.
    The full names and descriptions used in AD accounts are imported and stored with user objects in the BI platform.
    b. Specify an option for *Set priority of AD attribute binding relative to other attributes binding*.
    If the option is set to 1, AD attributes take priority when AD and other plugins (LDAP and SAP) are enabled. If the option is set to 3, attributes from other enabled plugins take priority. The bindings must be set to different values. Setting multiple authentication plugins to the same binding value leads to unexpected results.
12. In the *AD Group Options* area, configure AD group updates:
    a. Click *Schedule*.
    The *Schedule* dialog box appears.
    b. Select a recurrence from the *Run object* list.
    c. Set other schedule options and parameters as required.
    d. Click *Schedule*.

    The system schedules the update and runs it according to the schedule you specified. The next scheduled update for the AD group accounts is displayed under the *AD Group Options*.
13. In the *On-Demand AD Update* area, select an option to indicate whether to update AD groups or users (or neither) when you click *Update*:

- *Update AD Groups now*
  Select this option if you want to start updating all scheduled AD groups when you click *Update*. The next scheduled AD group update is listed under *AD Group Options*.
- *Update AD Groups and Aliases now*
  Select this option if you want to start updating all scheduled AD groups and user aliases when you click *Update*. The next scheduled updates are listed under *AD Group Options* and *AD Alias Options*.
- *Do not update AD Groups and Aliases now*
  No AD groups or user aliases will be updated when you click *Update*.

14. Click *Update*, and click *OK*.

9.4.6.3.1.3 To disable SiteMinder

If you want to prevent SiteMinder from being configured, or to disable it after it has been configured in the CMC, modify the web configuration file for BI launch pad.

9.4.6.3.1.3.1 To disable SiteMinder for Java clients

Context

In addition to disabling SiteMinder settings for the Windows AD security plugin, SiteMinder settings must be disabled for the BOE war file on your web application server.

Procedure

1. Go to the following directory in your BI platform installation:
   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Open the `global.properties` file.
3. Change `siteminder.enabled` to false

   ```
   siteminder.enabled=false
   ```

4. Save your changes and close the file.

Next Steps

The change takes effect only after `BOE.war` is redeployed on the machine running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy

to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

9.4.7 Troubleshooting Windows AD authentication

9.4.7.1 Troubleshooting your configuration

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Java SDK Kerberos configuration

9.4.7.1.1 To enable logging

Procedure

1. From the *Start* menu, select *Programs >Tomcat > Tomcat Configuration*
2. Click the *Java* tab.
3. Add the following options:

   ```
   -Dcrystal.enterprise.trace.configuration=verbose
   -sun.security.krb5.debug=true
   ```

   This will create a log file in the following location:

   ```
   C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
   ```

9.4.7.1.2 To test your Kerberos configuration

Procedure

Run the following command to test your Kerberos configuration, where `servant` is the service account and domain under which the CMS is running, and `password` is the password associated with the service account.

```
<InstallDirectory>\SAP BusinessObjects Enterprise XI
4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

For example:

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\
 servact@TESTM03.COM Password
```

Your domain and service principal name must exactly match the domain and service principal name in the Active Directory. If the problem persists, check whether you entered the same name; note that the name is case-sensitive.

9.4.7.1.3 Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to the BI platform. Despite this fact, they are unable to successfully log onto the CMC or BI launch pad with Windows AD authentication and Kerberos in the following format: `DOMAIN\ABC123`

This problem can happen when the user is set up in Active Directory with a UPN and SAM name that are not exactly the same. The following examples may cause a problem:

- The UPN is abc123@company.com but the SAM name is DOMAIN\ABC123.
- The UPN is jsmith@company but the SAM name is DOMAIN\johnsmith.

There are two ways to address this problem:

- Have users log in using the UPN name rather than the SAM name.
- Ensure the SAM account name and the UPN name are the same.

9.4.7.1.4 Pre-authentication error

A user who has previously been able to log on, can no longer log on successfully. The user will receive this error: Account Information Not Recognized. The Tomcat error logs reveal the following error: `"Pre-authentication information was invalid (24)"`

This can occur because the Kerberos user database didn't get a change made to UPN in AD. This may mean that the Kerberos user database and the AD information are out of sync.

To resolve this problem, reset the user's password in AD. This will ensure the changes are propagated correctly.

> **Note**
>
> This problem is not an issue with J2SE 5.0.

9.5 SAP authentication

9.5.1 Configuring SAP authentication

This section explains how to configure BI platform authentication for your SAP environment.

SAP authentication enables SAP users to log on to the BI platform using their SAP user names and passwords, without storing passwords in the BI platform. SAP authentication also allows you to preserve information about

user roles in SAP and to use role information in the platform to assign rights for performing administrative tasks or accessing content.

Accessing the SAP authentication application

You must provide the BI platform with information about your SAP system. A dedicated web application is accessible through the main BI platform administration tool, the Central Management Console (CMC). To access it from the home page of the CMC, click *Authentication*.

Authenticating SAP users

Security plug-ins expand and customize the ways in which the BI platform authenticates users. The SAP Authentication feature includes an SAP security plug-in (`secSAPR3.dll`) for the Central Management Server (CMS) component of the BI platform. This SAP security plug-in offers several key benefits:

- It acts as an authentication provider that verifies user credentials against your SAP system on behalf of the CMS. When users log on to the BI platform directly, they can choose SAP Authentication and provide their usual SAP user name and password. The BI platform can also validate Enterprise Portal logon tickets against SAP systems.
- It facilitates account creation by allowing you to map roles from SAP to BI platform user groups, and it facilitates account management by allowing you to assign rights to users and groups in a consistent manner within the BI platform.
- It dynamically maintains SAP role listings. So, once you map an SAP role to the platform, all users who belong to that role can log on to the system. When you make subsequent changes to the SAP role membership, you need not update or refresh the listing in the BI platform.
- The SAP Authentication component includes a web application for configuring the plug-in. You can access this application in the *Authentication* area of the Central Management Console (CMC).

9.5.2 Creating a user account for the BI platform

The BI platform system requires an SAP user account that is authorized to access SAP role membership lists and authenticate SAP. You need the account credentials to connect the BI platform to your SAP system. For general instructions on creating SAP user accounts and assigning authorizations through roles, see your SAP BW documentation.

Use transaction `SU01` to create a new SAP user account named `CRYSTAL`. Use transaction `PFCG` to create a new role named `CRYSTAL_ENTITLEMENT`. (These names are recommended but not required.) Change the new role's authorization by setting values for the following authorization objects:

Authorization object	Field	Value
Authorization for file access (S_DATASET)	Activity (ACTVT)	Read, Write (33, 34)
	Physical file name (FILENAME)	* (denotes All)
	ABAP program name (PROGRAM)	*
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)
User Master Maintenance: User Groups (S_USER_GRP)	Activity (ACTVT)	Create or Generate, and Display (03)
	User group in user master maintenance (CLASS)	* **Note** For greater security, you may prefer to explicitly list the user groups whose members require access to the BI platform.

Finally, add the `CRYSTAL` user to the `CRYSTAL_ENTITLEMENT` role.

→ Tip

If your system policies require users to change their passwords when they first log onto the system, log on now with the `CRYSTAL` user account and reset its password.

Note

Additional authorizations for the S_RFC object may be needed when certain performance enhancements have been enabled on the ABAP environment. These errors will be reported in the Role Import page, noting the Function to which authorization has failed:

Example: No RFC authorization for function module RFC_METADATA_GET.

Authorization object	Field	Value
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16

Authorization object	Field	Value
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY, and RFC_METADATA
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)

9.5.3 Connecting to SAP entitlement systems

Before you can import roles or publish BW content to the BI platform, you must provide information about the SAP entitlement systems to which you want to integrate. The BI platform uses this information to connect to the target SAP system when it determines role memberships and authenticates SAP users.

9.5.3.1 To add an SAP entitlement system

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link.

   The entitlement systems settings appear.

   > → Tip
   >
   > If an entitlement system is already displayed in the *Logical system name* list, click *New*.

3. In the *System* field, type the three-character System ID (SID) of your SAP system.
4. In the *Client* field, type the client number that the BI platform must use when it logs on to your SAP system. The BI platform combines your System and Client information, and adds an entry to the *Logical system name* list.
5. Ensure the *Disabled* check box is clear.

   > ⓘ Note
   >
   > Use the *Disabled* check box to indicate to the BI platform that a particular SAP system is temporarily unavailable.

6. Complete the *Message Server* and *Logon Group* fields as appropriate, if you have set up load balancing such that the BI platform must log on through a message server.

   > ⓘ Note
   >
   > You must make the appropriate entries in the `Services` file on your BI platform machine to enable load balancing, especially if your deployment is not on a single machine. Specifically you should

account for the machines hosting the CMS, the Web application server, as well as all machines managing your authentication accounts and settings.

7. If you have not set up load balancing (or if you prefer to have the BI platform log on directly to the SAP system), complete the *Application Server* and *System Number* fields as appropriate.
8. In the *User name*, *Password*, and *Language* fields, type the user name, password, and language code for the SAP account that you want the BI platform to use when it logs on to SAP.

   > ⓘ Note
   >
   > These credentials must correspond to the user account that you created for the BI platform.

9. Click *Update*.

Next Steps

If you add multiple entitlement systems, click the *Options* tab to specify the system that the BI platform uses as the default (that is, the system that is contacted to authenticate users who attempt to log on with SAP credentials but without specifying a particular SAP system).

9.5.3.2 To verify if your entitlement system was added correctly

Procedure

1. Click the *Role Import* tab.
2. Select the name of the entitlement system from the *Logical system name* list.

   If the entitlement system was added correctly, the *Available roles* list will contain a list of roles that you can choose to import.

   > → Tip
   >
   > If no roles are visible in the *Logical system name* list, look for error messages on the page. These may give you the information you need to correct the problem.

9.5.3.3 To temporarily disable a connection to an SAP entitlement system

Context

In the CMC, you can temporarily disable a connection between the BI platform and an SAP entitlement system. This may be useful to maintain the responsiveness of the BI platform in cases such as the scheduled down time of an SAP entitlement system.

Procedure

1. In the CMC, go to the *Authentication* management area.
2. Double-click the *SAP* link.
3. In the *Logical system name* list, select the system you want to disable.
4. Select the *Disabled* check box.
5. Click *Update*.

9.5.4 Setting SAP Authentication options

SAP Authentication includes a number of options that you can specify when integrating the BI platform with your SAP system. The options include:

- Enabling or disabling SAP authentication
- Specifying connection settings
- Linking imported users to BI platform license models.
- Configuring single sign-on to the SAP system

9.5.4.1 To set SAP Authentication options

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link, and click the *Options* tab.
3. Review and modify the following settings as needed:

Setting	Description
Enable SAP Authentication	Clear this check box to disable SAP Authentication.

Setting	Description
	Note To disable SAP Authentication for a specific SAP system, select that system's *Disabled* check box on the *Entitlement Systems* tab.
Content folder root	Specify where the BI platform should begin replicating the BW folder structure in the CMC and in BI launch pad. The default is `/SAP/2.0`, but you can change it to a different folder. If you want to change the value, you must change it both in the CMC and Content Administration Workbench.
Default system	Select a SAP entitlement system for the BI platform to contact to authenticate users who attempt to log on with SAP credentials but without specifying a particular SAP system. **Note** If you select a default system, users from that system do not have to enter a system ID or client when connecting from client tools, like Live Office or Universe Designer, using SAP authentication. For example, if SYS~100 is set as the default system, SYS~100/user1 could log on as user1 when SAP authentication is chosen.
Max. number of failed attempts to access entitlement system	Type the number of times that the BI platform should attempt to contact an SAP system to fulfill authentication requests. Setting the value to -1 allows the platform to attempt to contact the entitlement system an unlimited number of times. Setting the value to 0 limits the BI platform to making one attempt to contact the entitlement system. **Note** Use this setting with the *Keep entitlement system disabled [seconds]* option to configure how the BI platform handles SAP entitlement systems that are temporarily unavailable. The system uses the two options to determine when to stop communicating with an SAP system that is unavailable and when to resume communication with that system.
Keep entitlement system disabled [seconds]	Type the number of seconds for the BI platform to wait before resuming attempts to authenticate users against the SAP system.

Setting	Description
	For example, if *Max failed entitlement system accesses* is set to 3, the BI platform allows a maximum of three failed attempts to authenticate users against any SAP system. A fourth failed attempt stops the system from attempting to authenticate users against that system for the amount of time specified.
Max. concurrent connections per system	Specify how many connections to keep open in your SAP system at the same time. For example, if you type 2, the BI platform keeps two connections open to SAP.
Number of uses per connection	Specify how many operations to allow to the SAP system per connection. For example, if *Max concurrent connections per system* is set to 2 and *Number of uses per connection* is set to 3, once there are three logons on one connection, the BI platform closes and restarts that connection.
Concurrent users and *Named users*	Specify whether new user accounts will use concurrent user licenses or named user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small number of concurrent licenses can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users. Named user licenses are associated with users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. **Note** Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in. However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

Setting	Description
	Note The option you select does not change the number or type of user licenses installed in the BI platform. You must have the appropriate licenses available on your system.
Import Full Name, Email Address and other attributes	Specify a priority level for the SAP authentication plugin. The full names and descriptions used in the SAP accounts are imported and stored with user objects in the BI platform.
Set priority of SAP attribute binding relative to other attributes binding	Specifies a priority for binding SAP user attributes (full name and email address). If the option is set to 1, SAP attributes take priority in scenarios where SAP and other plugins (Windows AD and LDAP) are enabled. If the option is set to 3, attributes from other enabled plugins will take priority. The bindings must be set to different values. Setting multiple authentication plugins to the same binding value leads to unexpected results.

Set the following options to configure the SAP single sign-on service:

Setting	Description
System ID	The system identifier provided by the BI platform to the SAP system when performing the SAP single sign-on service.
Browse	Click to upload the `keystore` file generated to enable the SAP single sign-on. You can also manually enter the full path to the file.
Key Store Password	Provide the password required to access the `keystore` file.
Private Key Password	Provide the password required to access the certificate corresponding to the `keystore` file. The certificate is stored on the SAP system
Private Key Alias	Provide the alias required to access the `keystore` file.

4. Click *Update*.

9.5.4.2 To change the Content folder root

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link.
3. Click *Options* and type the name of the folder in *Content folder root* field.

   The folder name that you type here is the folder that you want the BI platform to begin replicating the BW folder structure from.
4. Click *Update*.
5. In the BW Content Administration Workbench, expand *Enterprise system*.
6. Expand *Available systems* and double-click the system that the BI platform is connecting to.
7. Click the *Layout* tab and in the *Content base folder*, type the folder that you want to use as the root SAP folder in the BI platform (for example, `/SAP/2.0/`).

9.5.5 Importing SAP roles

By importing SAP roles into the BI platform, you allow role members to log onto the system with their usual SAP credentials. In addition, single sign-on is enabled so that SAP users are logged on to the BI platform automatically when they access reports from within the SAP GUI or an SAP Enterprise Portal.

> **Note**
>
> There are often many requirements for enabling SSO. Some of these might include using a driver and application that are SSO-capable, and ensuring your server and web server are in the same domain.

For each role that you import, the BI platform generates a group. Each group is named with the following convention: **`<SystemID~ClientNumber@NameOfRole>`**. You can view the new groups in the *Users and Groups* management area of the CMC. You can also use these groups to define object security within the BI platform.

Consider three main categories of users when configuring the BI platform for publishing, and when importing roles to the system:

- BI platform administrators
  Enterprise administrators configure the system for publishing content from SAP. They import the appropriate roles, create necessary folders, and assign rights to those roles and folders in the BI platform.
- Content publishers
  Content publishers are those users who have rights to publish content into roles. The purpose of this category of user is to separate regular role members from those users with rights to publish reports.
- Role members
  Role members are users who belong to “content bearing” roles. That is, these users belong to roles to which reports are published. They have *View*, *View on Demand*, and *Schedule* rights for any reports published to the roles they are members of. However, regular role members cannot publish new content, nor can they publish updated versions of content.

You must import all content publishing and all content bearing roles to the BI platform prior to publishing for the first time.

> **Note**
>
> It is strongly recommended that you keep the activities of roles distinct. For example, while it is possible to publish from an administrator role, it is better practice to publish only from content publisher roles. Additionally, the function of content publishing roles is only to define which users can publish content. Thus, content publishing roles should not contain any content; content publishers should publish to content bearing roles that are accessible to regular role members.

9.5.5.1 To import SAP roles

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link.
3. On the *Options* tab, select *Concurrent users* or *Named users*, depending on your license agreement.

   This option does not change the number or type of user licenses that you have installed in the BI platform. You must have the appropriate licenses available on your system.
4. Click *Update*.
5. On the *Role Import* tab, select the appropriate entitlement system from the *Logical system name* list.
6. In the *Available roles* area, select the role(s) that you want to import, and click *Add*.
7. Click *Update*.

9.5.5.2 To verify that roles and users were imported correctly

Prerequisites

Before starting this task, take note of the user name and password of an SAP user who belongs to one of the roles that you mapped to the BI platform.

Procedure

1. For Java BI launch pad, go to **`http://<webserver>:<portnumber>/BOE/BI`**.

   Replace `<webserver>` with the name of the web server and `<portnumber>` with the port number for the BI platform. You may need to ask your administrator for the name of the web server, the port number, or the URL to enter.

2. From the *Authentication Type* list, select *SAP*.

> **Note**
>
> By default, the *Authentication Type* list is hidden in BI launch pad. If the list is not visible, ask your system administrator to enable the *Authentication Type* list in the `BIlaunchpad.properties` file and then restart the app server.

3. Enter the SAP system and system client that you want to log on to.
4. Enter the user name and password of a mapped user.
5. Click *Log On*.

   You are logged on to BI launch pad as the selected user.

9.5.5.3 Updating SAP roles and users

After enabling SAP authentication, it is necessary to schedule and run regular updates on mapped roles that have been imported into the BI platform. This will ensure that your SAP role information is accurately reflected in the platform.

There are two options for running and scheduling updates for SAP roles:

- Update roles only: Using this option will only update the links between the currently mapped roles that have been imported in the BI platform. It is recommended that you use this option if you expect to run frequent updates, and you have concerns over system resource usage. No new user accounts will be created if you only update SAP roles.
- Update roles and aliases: This option not only updates links between roles but will also create new user accounts in the BI platform for user aliases added to roles in the SAP system.

> **Note**
>
> If you have not specified to automatically create user aliases for updates when you enabled SAP authentication, no accounts will be created for new aliases.

9.5.5.3.1 To schedule updates for SAP roles

Context

After you map roles in the BI platform, you must specify how the system updates the roles.

Procedure

1. Click the *User Update* tab.

2. Click *Schedule* in the *Update Roles Only* section or the *Update Roles and Aliases* area.

> → Tip
>
> To immediately run an update, click *Update Now*.

> → Tip
>
> Use the *Update Roles Only* option if you would like frequent updates and have concerns about system resources. It takes the system longer to update both roles and aliases.

The *Recurrence* dialog box appears.

3. Select an option from the *Run Object* list and provide all the requested scheduling information in the fields provided.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify the time it will start and the start and end dates.
Daily	The update will run every day or every <n> days (where <n> is the number of days you specify). You can specify the time it will start and the start and end dates.
Weekly	The update will run every week, once a week or several times a week. You can specify on which days it will run, the time it will start, and the start and end dates.
Monthly	The update will run every month or every several months. You can specify the time it will start and the start and end dates.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as and a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as and a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as and a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule*.
The date of the next scheduled role update appears on the *User Update* tab.

> → Tip
>
> To cancel the next scheduled update, click *Cancel Scheduled Updates* in the *Update Roles Only* area or *the Update Roles and Aliases* area.

9.5.6 Configuring Secure Network Communication (SNC)

This section describes how to configure SNC as part of the process of setting up SAP authentication to the BI platform.

For more information, see SAP Note 1396213.

Before setting up trust between the SAP and BI platform systems, you must ensure the SIA is configured to start and run under an account that has been set up for SNC. You must also configure your SAP system to trust the BI platform.

Related Information

SAP Server-Side Trust Overview [page 335]

9.5.6.1 SAP Server-Side Trust Overview

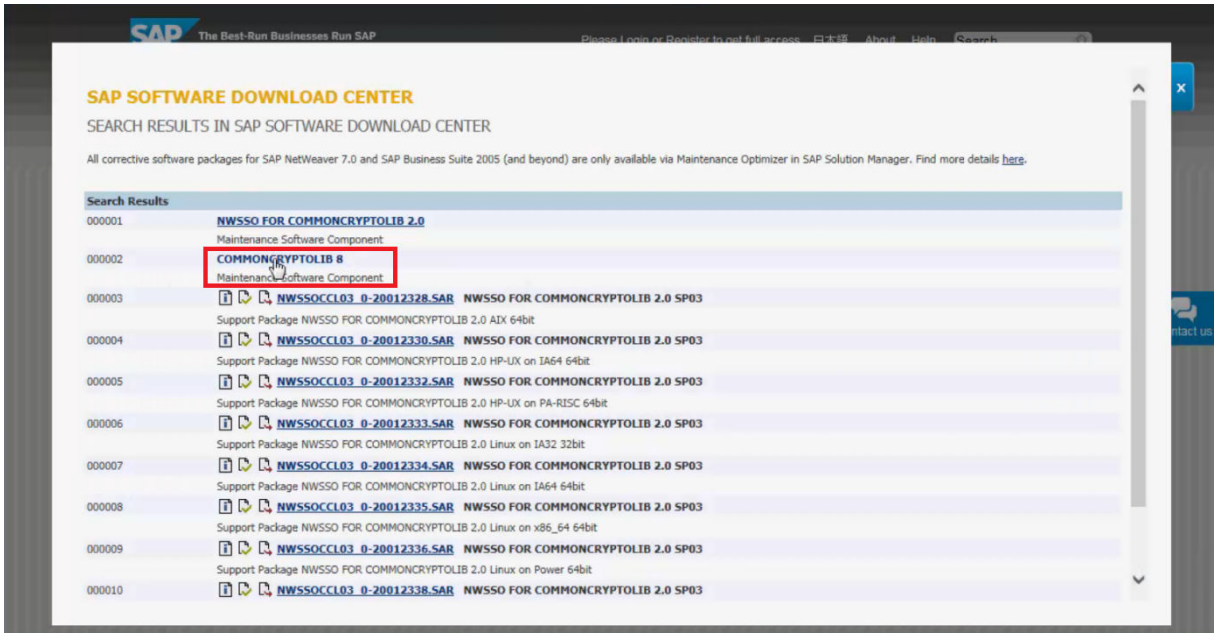
This section provides procedures for configuring server-side trust between SAP Web Application Servers (version 6.20 and up) and SAP BusinessObjects Business Intelligence platform. You need to set up server-side trust if you are using multi-pass report bursting (for publications where the report query depends on the context of the user).

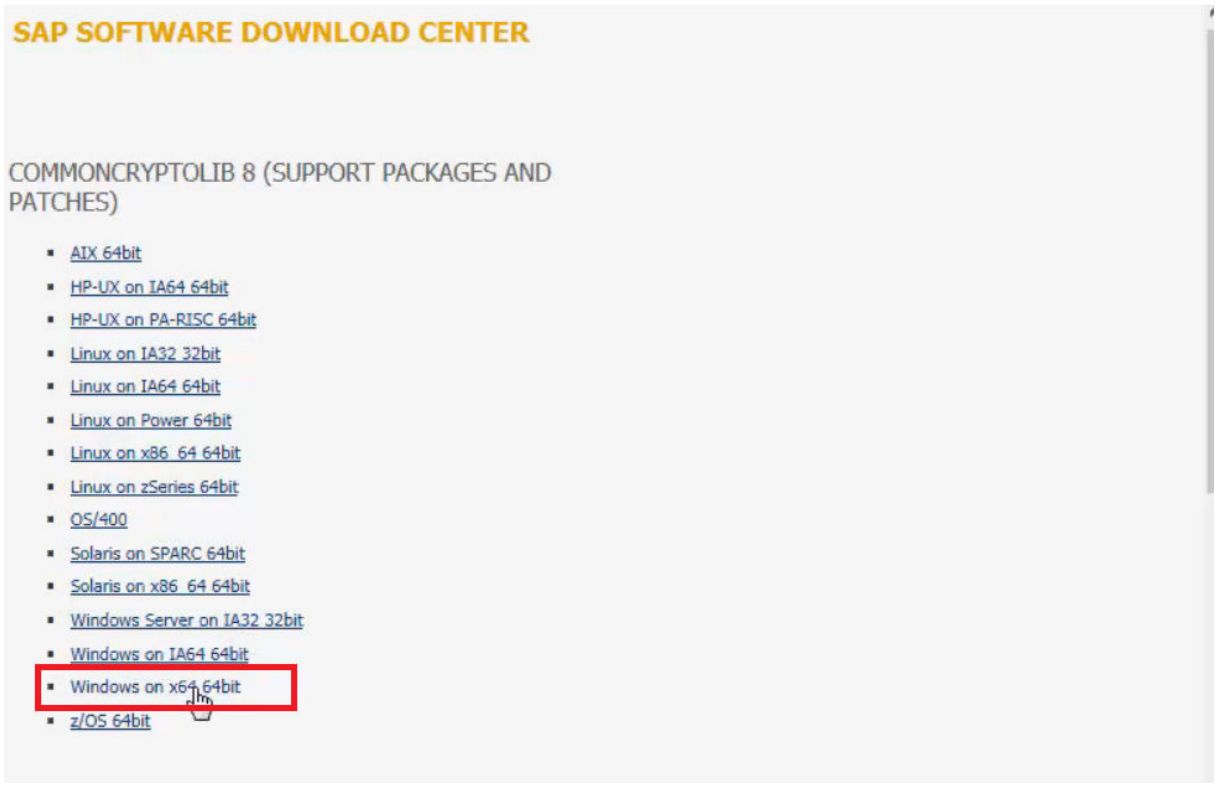
Server-side trust involves password-less impersonation. To impersonate an SAP user without providing a password, a user must be identified with SAP using a more secure method than a regular username and password. (An SAP user with the SAP_ALL authorization profile cannot impersonate another SAP user without knowing that user's password.)

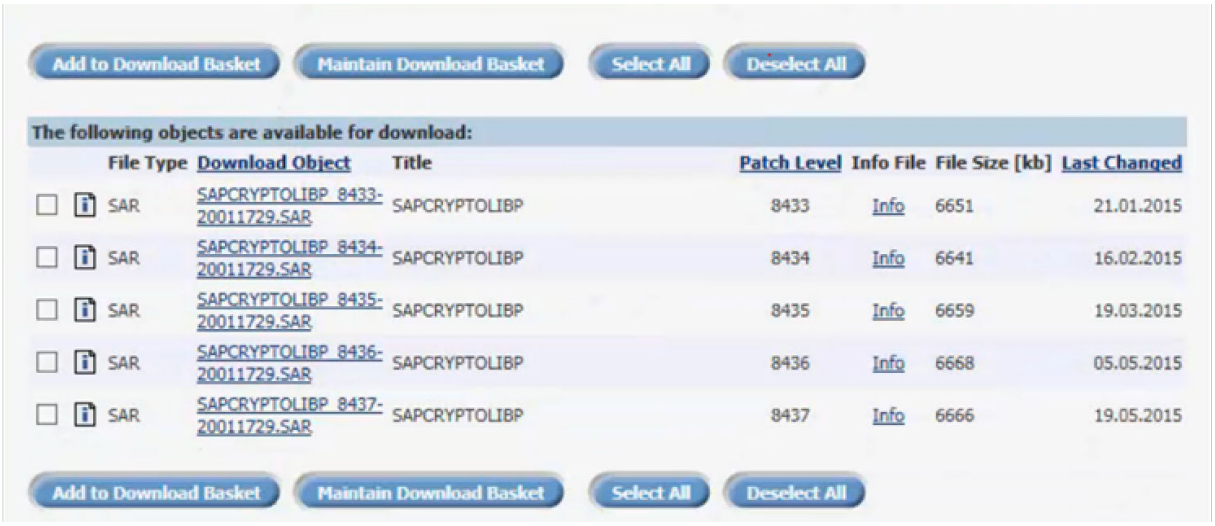
Enabling server-side trust using the SAP crypto library

To enable server-side trust for the BI platform using the SAP Cryptographic Library, you must run the relevant servers under credentials that are authenticated using a registered Secure Network Communication (SNC) provider. These credentials are configured within SAP to be allowed to impersonate without a password. For the BI platform, you need to run the servers involved in report-bursting under these SNC credentials, such as the Adaptive Job Server.

You need 32-bit SNC binaries for 32-bit processes; 64-bit SNC binaries for 64-bit processes. An SAP Cryptographic Library is installed along with the BI platform. Note that the SAP Cryptographic Library can be used only for setting up server-side trust. The Cryptographic Library is available for Windows and UNIX.


SAP
The Best-Run Businesses Run SAP
SAP SOFTWARE DOWNLOAD CENTER
SEARCH RESULTS IN SAP SOFTWARE DOWNLOAD CENTER
All corrective software packages for SAP NetWeaver 7.0 and SAP Business Suite 2005 (and beyond) are only available via Maintenance Optimizer in SAP Solution Manager. Find more details here.
Search Results
000001 NWSSO FOR COMMONCRYPTOLIB 2.0
Maintenance Software Component
000002 COMMONCRYPTOLIB 8
Maintenance Software Component
000003 NWSSOCCL03_0-20012328.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 AIX 64bit
000004 NWSSOCCL03_0-20012330.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 HP-UX on IA64 64bit
000005 NWSSOCCL03_0-20012332.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 HP-UX on PA-RISC 64bit
000006 NWSSOCCL03_0-20012333.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on IA32 32bit
000007 NWSSOCCL03_0-20012334.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on IA64 64bit
000008 NWSSOCCL03_0-20012335.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on x86_64 64bit
000009 NWSSOCCL03_0-20012336.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on Power 64bit
000010 NWSSOCCL03_0-20012338.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03


SAP SOFTWARE DOWNLOAD CENTER
COMMONCRYPTOLIB 8 (SUPPORT PACKAGES AND PATCHES)
AIX 64bit
HP-UX on IA64 64bit
HP-UX on PA-RISC 64bit
Linux on IA32 32bit
Linux on IA64 64bit
Linux on Power 64bit
Linux on x86_64 64bit
Linux on zSeries 64bit
OS/400
Solaris on SPARC 64bit
Solaris on x86_64 64bit
Windows Server on IA32 32bit
Windows on IA64 64bit
Windows on x64 64bit
z/OS 64bit



For more information about the Cryptographic Library, see SAP notes 711093, 597059 and 397175 on the SAP web site.

The SAP server and the BI platform need to be assigned certificates that prove their identities to each other. Each server will have its own certificate and a list of certificates for trusted parties. To configure server-side trust between SAP and the BI platform, you need to create a password-protected set of certificates called a Personal Security Environment (PSE). This section describes how to set up and maintain the PSEs, and how to securely associate them with BI platform processing servers.

SAP BusinessObjects BI platform server responsibilities

Specific BI platform servers are relevant to the SAP integration in terms of single sign-on (SSO). The following table lists these servers, and their areas of responsibility.

Server	Areas of responsibility
Web Application Server	SAP Authentication role list
BW Publisher Service	Crystal Reports Dynamic Parameter pick lists and personalization
CMS	Password, ticket, checking role membership, and user lists
Page Server	Crystal Reports view on demand
Job Server	Scheduling Crystal Reports
Web Intelligence Processing Server	Viewing and scheduling Web Intelligence reports and List of Values (LOV) prompts
Multi-Dimensional Analysis Service	Analysis

9.5.6.2 Configuring SAP for server-side trust

Server-side trust applies only to Crystal reports and Web Intelligence reports that are based on Universes (`.unv`). You must set up SNC for use with the BI platform. For more information or for troubleshooting assistance, consult the SAP documentation provided with your SAP server.

9.5.6.2.1 To configure SAP for server-side trust

Procedure

1. Ensure that you have SAP administrator's credentials for within SAP and for the machine running SAP, and administrator's credentials for the BI platform and the machine (or machines) it is running on.
2. On the SAP machine, ensure that the SAP Cryptographic Library and the SAPGENPSE tool are located in the `<DRIVE>:\usr\sap\<SID>\SYS\exe\run\` directory (on Windows).
3. Create an environment variable named **`<SECUDIR>`** that points to the directory where the ticket resides.

   > ⓘ Note
   >
   > This variable must be accessible to the user under which SAP's *disp+work* process runs.

4. In the SAP GUI, go to transaction RZ10 and change the instance profile in *Extended maintenance* mode.
5. In profile edit mode, point SAP profile variables to the Cryptographic Library and give the SAP system a Distinguished Name (DN). These variables should follow the LDAP naming convention:

Tag	Meaning	Description
`CN`	Common Name	The everyday name of the certificate proprietor.
`OU`	Organizational Unit	PG for Product Group, for example.
`O`	Organization	The name of the organization for which the certificate was issued.
`C`	Country	The country where the organization is located.

   For example, for R21: **`p:CN=R21, OU=PG, O=BOBJ, C=CA`**

   > ⓘ Note
   >
   > The prefix **`p:`** is for the SAP Cryptographic Library. It is required when referring to the DN within SAP, but will not be visible when examining certificates in STRUST or using SAPGENPSE.

6. Enter the following profile values, substituting for your SAP system where necessary:

Profile variable	Value
`ssf/name`	**`SAPSECULIB`**

Profile variable	Value
ssf/ssfapi_lib	Full path to sapcrypto lib
sec/libsapsecu	Full path to sapcrypto lib
snc/gssapi_lib	Full path to sapcrypto lib
snc/identity/as	Your SAP system's DN

7. Restart your SAP instance.
8. When the system is running again, log on and go to transaction STRUST, which should now have additional entries for SNC and SSL.
9. Right-click the SNC node and click *Create*.
   The identity you specified in RZ10 should now appear.
10. Click *OK*.
11. To assign a password to the SNC PSE, click the lock icon.

> **Note**
>
> Do not lose this password. You will be prompted for it by STRUST every time you view or edit the SNC PSE.

12. Save the changes.

> **Note**
>
> If you do not save your changes, the application server will not start again when you enable SNC.

13. Return to transaction RZ10 and add the remainder of the SNC profile parameters:

Profile variable	Parameter
snc/accept_insecure_rfc	**1**
snc/accept_insecure_r3int_rfc	**1**
snc/accept_insecure_gui	**1**
snc/accept_insecure_cpic	**1**
snc/permit_insecure_start	**1**
snc/data_protection/min	**1**
snc/data_protection/max	**3**
snc/enable	**1**

The minimum protection level is set to authentication only (1) and the maximum is privacy (3). The **snc/data_protection/use** value defines that only authentication is to be used in this case, but could also be (2) for integrity, (3) for privacy and (9) for maximum available. The **snc/accept_insecure_rfc**, **snc/accept_insecure_r3int_rfc**, **snc/accept_insecure_gui**, and **snc/accept_insecure_cpic** values set to (1) ensure that previous (and potential unsecure) communication methods are still permitted.

14. Restart your SAP system.

Next Steps

You must now configure the BI platform for server-side trust.

9.5.6.3 Configuring the BI platform for server-side trust

The following procedures need to be performed in order to configure the BI platform for server-side trust. Note that these steps are Windows-based, but because the SAP tool is a command line tool, the steps are very similar on Unix.

1. Set up the environment
2. Generate a Personal Security Environment (PSE)
3. Configure the BI platform servers
4. Configure PSE access
5. Configure SAP Authentication SNC settings
6. Set up SAP dedicated server groups

Related Information

To set up the environment [page 340]
To generate a PSE [page 341]
To configure BI platform servers [page 343]
To configure PSE access [page 343]
To configure SAP authentication SNC settings [page 344]
Using server groups [page 346]

9.5.6.3.1 To set up the environment

Prerequisites

The BI platform includes a default SAP Cryptographic Library. If you use the default library, you need to perform only the last two steps: create a subfolder, and add an environment variable. Otherwise, to configure a custom copy of the SAP Cryptographic Library, perform all of the steps.

The default SAP Cryptographic Library can be found at this location:

- Windows: `<INSTALLDIR>\sap\sapcrypto.dll`
- Unix: `<INSTALLDIR>/sap/libsapcrypto.so`

Before you begin, ensure that:

- The SAP Cryptographic Library has been expanded on the host on which BI platform processing servers run.

- The appropriate SAP systems have been configured to use SAP Cryptographic Library as the SNC provider.

Context

Before PSE maintenance can begin, you need to set up the library, tool, and environment where PSEs are stored.

Procedure

1. Copy the SAP Cryptographic Library (including the PSE maintenance tool) to a folder on the machine running the BI platform.

   For example: `C:\Program Files\SAP\Crypto`.
2. Add the folder to the `<PATH>` environment variable.
3. Add a system-wide environment variable `<SNC_LIB>` that points to the Cryptographic Library.

   For example: `C:\Program Files\SAP\Crypto\sapcrypto.dll`

   > **Note**
   >
   > The maximum path length is 100 characters.
4. Create a subfolder named **`sec`**.

   For example: `C:\Program Files\SAP\Crypto\sec`.
5. Add a system-wide environment variable `<SECUDIR>` that points to the **`sec`** folder.

Related Information

Configuring SAP for server-side trust [page 338]

9.5.6.3.2 To generate a PSE

Context

SAP accepts a BI platform server as a trusted entity when the relevant BI platform servers have a PSE and the PSE is associated with SAP. This “trust” between SAP and BI platform components is established by sharing the public version of each other's certificates. The first step is to generate a PSE for the BI platform that automatically generates its own certificate.

Procedure

1. Open a command prompt and run **`sapgenpse.exe gen_pse -a sha256WithRsaEncryption -s 2048 -v -p BOE.pse`** from within the Cryptographic Library folder.
2. Choose a PIN and the DN you want for your BI platform system.

   For example, **`CN=MyBOE01, OU=PG, O=BOBJ, C=CA`**.

   You now have a default PSE, with its own certificate.
3. Use the following command to export the certificate in the PSE:

   `sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>`
4. In the SAP GUI, go to transaction STRUST and open the system PSE associated with your SAP system.

   You may be prompted for the password you have already assigned to this system PSE.
5. Import the `<MyBOECert.crt>` file created earlier by clicking the "Import Certificate" button at the bottom left of the STRUST transaction screen.

   The certificates from SAPGENPSE are Base64-encoded. Make sure you select Base64 when importing them.
6. To add the BI platform certificate to the SAP server's PSE certificate list, click the *Add to certificate list* button.
7. Save your changes in STRUST.
8. Click the *Export* button and provide a file name for the certificate.

   For example, **`MySAPCert.crt`**.

   > **Note**
   >
   > The format should remain Base64.
9. Go to transaction SNC0.
10. Add a new entry, where:
    - The System ID is arbitrary but reflects your BI platform system.
    - The SNC name should be the DN (prefixed by **`p:`**) that you provided when you created your BI platform PSE (in step 2).
    - The *Entry for RFC activated* and *Entry for ext. ID activated* check boxes are both selected:
11. To add the exported certificate to the BI platform PSE, run the following command on the command prompt:

    `sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse`

Results

The SAP Cryptographic Library is installed on the BI platform machine. You have created a PSE that will be used by BI platform servers to identify themselves to SAP servers. SAP and the BI platform PSE have exchanged certificates. SAP permits entities with access to the BI platform PSE to perform RFC calls and password-less impersonation.

Related Information

To configure BI platform servers [page 343]

9.5.6.3.3 To configure BI platform servers

Context

After you generate a PSE for the BI platform, you must configure an appropriate server structure for SAP processing. The following procedure creates a node for SAP processing servers, so that you can set operating system credentials on the node level.

> **Note**
>
> In this version of the BI platform, servers are no longer configured in the Central Configuration Manager (CCM). Instead, a new Server Intelligence Agent (SIA) must be created.

Procedure

1. In the CCM, create a new node for SAP processing servers.
   Give the node an appropriate name such as **`SAPProcessor`**.
2. In the CMC, add the processing servers you need to the new node, then start the new servers.

9.5.6.3.4 To configure PSE access

Context

After you configure the BI platform node and servers, you need to configure PSE access using the SAPGENPSE tool.

Procedure

1. Run the following command from the command prompt:

   ```
   sapgenpse.exe seclogin -p SBOE.pse
   ```

> **Note**
>
> You will be prompted for the PSE PIN. If you run the tool under the same credentials used by your BI platform SAP processing servers, you do not need to specify a user name.

2. To verify that the single sign-on (SSO) link is established, list the contents of the PSE using the following command:

   ```
   sapgenpse.exe maintain_pk -l
   ```

   The results should look similar to the following:

   ```
   C:\Documents and
   Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:\Documents and Settings\username\My
   Documents\snc\sec\bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***
   1. ------------------------------------------------------------
              Version:                  0 (X.509v1-1988)
              SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
              IssuerName:               CN=R21Again, OU=PG, O=BOBJ, C=CA
              SerialNumber:             00
              Validity  -  NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                  NotAfter:
   Thu Dec 31 16:00:01 2037 (380101000001Z)
              Public Key Fingerprint:   851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
              SubjectKey:               Algorithm RSA (OID
   1.2.840.113549.1.1.1), NULL
   C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
   ```

   You should not be prompted again for the PSE PIN after a successful **seclogin** command.

> **Note**
>
> If you encounter PSE access problems, use the `-O` argument to specify PSE access. For example, to grant PSE access to a specific user in a specific domain, on Windows, type this command:
>
> ```
> sapgenpse seclogin -p SBOE.pse -O SYSTEM
> ```

9.5.6.3.5 To configure SAP authentication SNC settings

Context

After you configure PSE access, you must configure SAP authentication settings in the CMC.

Procedure

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link.

The entitlement systems settings appear.

3. Click the *SNC Settings* tab on the *SAP Authentication* page.
4. Select your entitlement system from the *Logical system name* list.
5. Select *Enable Secure Network Communication (SNC)* under *Basic Settings*.
6. Select the *Use Default* option to accept the default path for the library, or select the *Define Custom Path* option to choose a different location.
7. Select a level of protection under *Quality of Protection*.

   For example, select *Authentication*.

   > **Note**
   >
   > Do not exceed the level of protection configured on the SAP system. The level of protection is customizable and is determined by your organization's needs and the capabilities of their SNC library.

8. Enter the SNC name of the SAP system under *Mutual authentication settings*.

   The SNC name format depends on the SNC library. Using the SAP cryptography library, the distinguished name recommendation is that it follows LDAP naming conventions and has `p:` as its prefix.
9. Confirm that the SNC name of the credentials under which the BI platform servers run appears in the *SNC name of Enterprise system* box.

   When several SNC names are configured, this field should be left blank.
10. Provide the DNs of the SAP system and the BI platform PSE.

9.5.6.3.6 Using server groups

Unless the processing (Crystal Reports or Web Intelligence) servers are running under credentials that have access to the PSE, you must create a specific server group containing only these servers along with the required supporting servers. For more information and descriptions of the various BI platform servers, see the "Architecture" chapter.

There are three options to choose from when configuring content processing servers for your SAP content:

1. Maintain a single SIA, including all BI platform servers, running under credentials that have access to the PSE. This is the simplest option - no server groups need to be created. This approach is the least secure in that an unnecessary number of servers have access to the PSE.
2. Create a second SIA with access to the PSE and add to it the Crystal Reports or Web Intelligence processing servers. Delete the duplicated servers from the original SIA. No server groups need to be created but fewer servers have access to the PSE.
3. Create a SIA exclusively for use for SAP with access to the PSE. Add to it the Crystal Reports or Web Intelligence processing servers. With this option, only SAP content should run on these servers, and more importantly, SAP content should run only on these servers. Since in this scenario content needs to be directed to certain servers, you must create server groups for the SIA.

Guidelines for using a server group

The server group needs to reference the SIA used exclusively to handle SAP content. In addition, the server group needs to reference the following servers:

- Adaptive Servers
- Adaptive Job Servers

All SAP content, Web Intelligence documents, and Crystal reports need to be associated with the server group using the strictest association; that is, that they must run on servers in the group. When this association is done on an object level, the server group setting should be propagated into settings for both direct scheduling as well as for publications.

To prevent other (non-SAP) content from processing on the SAP-specific processing servers, you should create another server group that includes all the servers under the original SIA. It is recommended that you set up a strict association between this content and the non-SAP server group.

9.5.6.4 Configuring multi-pass publications

Troubleshooting multi-pass publications

If you encounter problems with multi-pass publications, enable tracing for the Crystal Reports (CR) or Multidimensional Data Access (MDA) drivers for SAP and look at the logon string used for each job or recipient. These logon strings should resemble the following:

```
SAP: Successfully logged on to SAP server.
```

```
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:\WINDOWS\System32\sapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3
EXTIDTYPE=UN
```

The logon string must have the appropriate **EXTIDTYPE=UN** (for username) and **EXTIDDATA** should be the SAP username of the recipient. In this example, the logon attempt was successful.

9.5.6.5 Workflow for integrating with Secure Network Communication

The BI platform supports environments that implement Secure Network Communication (SNC) for authentication and data encryption between SAP components. If you have deployed the SAP Cryptographic Library (or another external security product that uses the SNC interface) you must set some additional values to integrate the BI platform effectively within your secured environment.

To configure the platform to use your secure network communication, you must complete the following tasks:

1. Configure BI platform servers to start and run under an appropriate user account.
2. Configure the SAP system to trust your BI platform system.
3. Configure the SNC settings in the SNC link in the Central Management Console.
4. Import SAP roles and users into the BI platform.

Related Information

Importing SAP roles [page 331]

9.5.6.6 To configure SNC settings in the Central Management Console

Prerequisites

Before you can configure SNC settings, you must add a new entitlement system to the BI platform, ensure that the SNC library file is in a known directory, and create an environment variable `<RFC_LIB >`to point to the file.

Procedure

1. Click the *SNC Settings* tab on the *SAP Authentication* page.
2. Select your entitlement system from the *Logical system name* list.

3. Select *Enable Secure Network Communication (SNC)* under *Basic Settings*.
4. If you are configuring SAP authentication for the consumption of `.unx` Universes or OLAP BICS connections and plan to use STS, select the *Prevent insecure incoming RFC connections* check box.
5. Select the *Use Default* option to accept the default path for the library, or select the *Define Custom Path* option to choose a different location.

   The web application server and the CMS must be on the same OS type with the same path to the crypto library.
6. Select a level of protection under *Quality of Protection*.

   For example, select *Authentication*.

   > **Note**
   >
   > The level of protection is customizable and is determined by your organization's needs and the capabilities of their SNC library.
7. Enter the SNC name of the SAP system under *Mutual authentication settings*.

   The SNC name format depends on the SNC library. Using the SAP cryptography library, the distinguished name recommendation is that it follows LDAP naming conventions and has `p:` as its prefix.
8. Confirm that the SNC name of the credentials under which BI platform servers run appears in the *SNC name of Enterprise system* box.
9. Click *Update.*

Related Information

Connecting to SAP entitlement systems [page 325]

9.5.6.7 To associate the entitlement user with an SNC name

Procedure

1. Log on to your SAP BW system and execute the transaction `SU01`.

   The User Maintenance: Initial Screen opens.
2. In the *User* field, type the name of the SAP account designated as the entitlement user and then click *Change* on the toolbar.

   The Maintain User screen opens.
3. Click the SNC tab.
4. In the *SNC name* field, type the `SNC USER ACCOUNT` you entered in step 2 above.
5. Click *Save*.

9.5.6.8 To add a system ID to the SNC Access Control list

Procedure

1. Log on to your SAP BW system and execute the transaction `SNC0`.

   The Change View "SNC: Access Control List (ACL) for Systems: Overview" screen opens.
2. Click *New Entries* on the toolbar.

   The New Entries: Details of Added Entries screen opens.
3. Type the name of your BI platform machine in the *System ID* field.
4. Type `p:<SNC USER NAME>` in the *SNC user name* field, where `SNC USER NAME` represents the account you used when configuring the BI platform servers.

   > **Note**
   >
   > If your SNC provider is gssapi32.dll, use uppercase letters when indicating the SNC USER NAME. You must include the domain name when specifying the user account. For example: domain\username.
5. Select *Entry for RFC activated* and *Entry for ext. ID activated*.
6. Clear all other options and click *Save*.

9.5.7 Setting up single sign-on to the SAP system

Different BI platform client and back-end services interact with SAP NetWeaver ABAP back-end systems in an integrated environment. It is useful to set up single sign-on from the BI platform to these (typically BW) back-end systems. After an ABAP system is configured as an external authentication system, proprietary SAP tokens are used to provide a mechanism that supports single sign-on for all BI platform clients and services connecting to SAP NetWeaver ABAP systems.

For more information, see support note 1670073.

To enable single sign-on to the SAP system, you need to create a `keystore` file and a corresponding certificate. Use the `keytool` command line program to generate the file and the certificate. By default the keytool program is installed in the `sdk/bin` directory for each platform.

The certificate needs to be added to your SAP ABAP BW system, and to the BI platform using the CMC.

> **Note**
>
> The SAP authentication plugin must be configured before you can set up single sign-on to the database used by SAP BW.

9.5.7.1 To generate the keystore file

Context

The topic contains instructions to use Java Keytool for generating keystore files. The table below lists the default locations of the Java Keytool:

Platform	Default location
Windows	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\ win64_x64\sapjvm\bin`
Linux	`sap_bobj/enterprise_xi40/linux_x64/ sapjvm/bin/keytool`

Procedure

1. Go to Java Keytool's default location and launch Command Prompt.
2. Run the Java Keytool for generating keystore.
   a. Go to <INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.
   b. Run the command:
      - Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`
      - Linux: `*/sap_bobj/enterprise_xi40/java/lib>/sap_bobj/enterprise_xi40/ linux_x64/sapjvm/bin/keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`

> → Tip
>
> To override the default values, run the tool together with the -? parameter. The following message is displayed:

> {·} Sample Code

```
Usage: keytool -genkey <options>
        -keystore <filename(keystore.p12)>
        -alias <key entry alias(mywin)>
        -storepass <keystore password (admin1)>
        -dname <certificate subject DN(CN=palmtree)>
        -validity <number of days (365)>
        -cert <filename (cert.der)>
         (No certificate is generated when importing a keystore)
        -importkeystore <filename>
```

You can use the parameters to override the default values.

> **Note**
>
> You must use Java Keytool as a replacement of PKCS12 tool to generate keystore. Refer 2524775 for more information.

9.5.7.2 To export the public key certificate

Context

You need to create and export a certificate for the keystore file.

Procedure

1. Launch a command prompt and navigate to the directory where the keytool program is located
2. To export a key certificate for the keystore file use the following command:

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

Replace <keystore> with the name of the keystore file.
Replace <filename> with the name of the certificate.
Replace <alias> with the alias used to create the keystore file.

3. When prompted, enter the password you provided for the keystore file.

Results

You now have a keystore file and a certificate in the directory where the keytool program is located.

9.5.7.3 Importing the certificate file into the target ABAP SAP system

Prerequisites

You need a key store file and an associated certificate for your BI platform deployment to perform the following task.

Context

> **Note**
>
> This action can only be performed on an ABAP SAP system.

Procedure

1. Connect to your SAP ABAP BW system using the SAP GUI.

   > **Note**
   >
   > You should connect as a user with administrative privileges.

2. Execute STRUSTSSO2 in the SAP GUI.
   The system is prepared for importing the certificate file.
3. Go to the *Certificate* tab.
4. Ensure the *Use Binary option* check box is selected.
5. Click the file path button to point to the location where the certificate file is located.
6. Click the green check mark.
   The certificate file is uploaded.
7. Click *Add to Certificate List*.
   The certificate is displayed in the Certificate List.
8. Click *Add to ACL* and specify a SystemID and Client.

   The system ID must be the same used to identify the BI platform system to SAP BW.

   The certificate is added to the Access Control List (ACL). The client should be specified as “000”.
9. Save your setting and exit.
   The changes are saved in the SAP system.

9.5.7.4 To set up single sign-on to the SAP database in the CMC

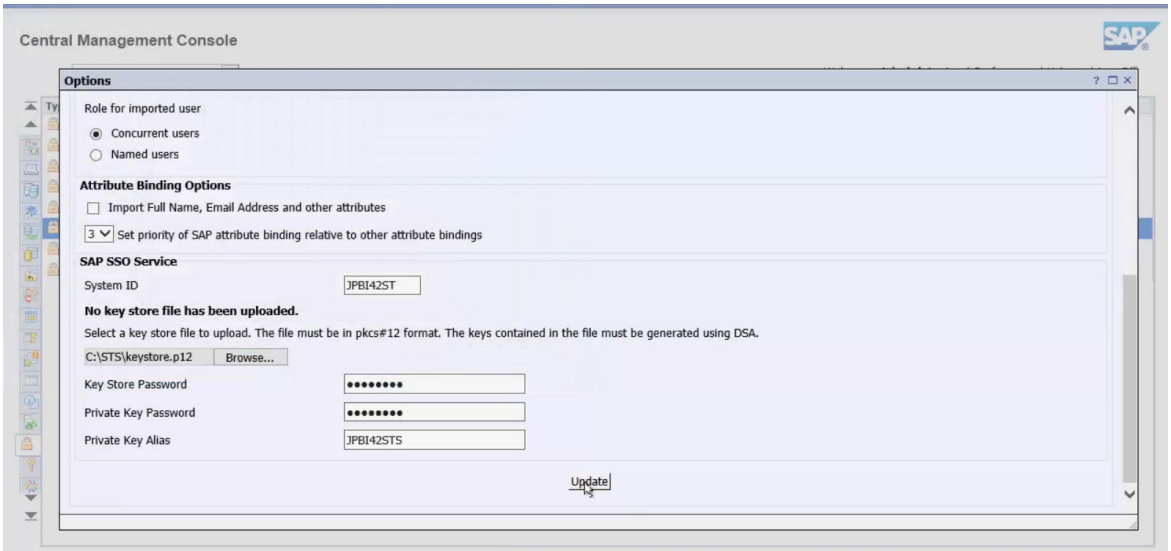
Prerequisites

To perform the following procedure you need to access the SAP security plugin using an administrator account.

Procedure

1. Go to the *Authentication* management area of the CMC.

2. Double-click the *SAP* link and then click the *Options* tab.



If no certificate has been imported the following message should be displayed in the *SAP SSO Service* section:

```
No key store file has been uploaded
```

3. Specify the System ID for your BI platform system in the field provided.

   This should be identical to the value used when importing the certificate in the target SAP ABAP system.

4. Click the *Browse* button to point to the key store file.
5. Provide the following required details:

Field	Required information
Key Store Password	Provide the password required to access the key store file. This password was specified when creating the key store file.
Private Key Password	Provide the password required to access the certificate corresponding to the key store file. This password was specified when creating the certificate for the key store file.
Private Key Alias	Provide the alias required to access the key store file. This alias was specified when creating the key store file.

6. Click *Update* to submit your settings.

   Once the settings are submitted successfully, the following message is displayed under the SystemID field:

```
Key store file have been uploaded
```

9.5.7.5 To add the Security Token Service to the Adaptive Processing Server

Context

In a clustered environment, Security Token Services are added separately to each Adaptive Processing Server.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click *Core Services*.
   The list of servers appears under *Core Services*.
3. Right-click the Adaptive Processing Server and select *Stop Server*.
   Do not proceed until the server state is Stopped.
4. Right-click the Adaptive Processing Server and select *Select Services*.
   The *Select Services* dialog box appears.
5. Use the *add* button to move Security Token Service from the *Available services* list to the *Services* list.
6. Click *OK*.
7. Restart the Adaptive Processing Server.

9.5.8 Configuring SSO for SAP Crystal Reports and SAP NetWeaver

By default, the BI platform will be configured to allow SAP Crystal Reports users to access SAP data using Single Sign-on (SSO).

9.5.8.1 To deactivate SSO for SAP NetWeaver and SAP Crystal Reports

Procedure

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select one of the following drivers:

Driver	Display name
Operational Data Store driver	*crdb_ods*
Open SQL driver	*crdb_opensql*
Infoset driver	*crdb_infoset*
BW MDX Query driver	*crdb_bwmdx*

5. Click *Remove*.
6. Click *Save & Close*.
7. Restart SAP Crystal Reports.

9.5.8.2 To reactivate SSO for SAP NetWeaver and SAP Crystal Reports

Context

Follow the steps below to reactivate SSO for SAP NetWeaver (ABAP) and SAP Crystal Reports.

Procedure

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Under *Use SSO context for database logon* type:

`crdb_ods`	To activate the ODS driver
`crdb_opensql`	To activate the Open SQL driver
`crdb_bwmdx`	To activate the SAP BW MDX Query driver
`crdb_infoset`	To activate the InfoSet driver

5. Click *Add*.
6. Click *Save & Close*.
7. Restart SAP Crystal Reports.

9.6 PeopleSoft authentication

9.6.1 Overview

To use your PeopleSoft Enterprise data with the BI platform, you must provide the program with information about your deployment. This information allows the BI platform to authenticate users so that they can use their PeopleSoft credentials to log on to the program.

9.6.2 Enabling PeopleSoft Enterprise authentication

To allow PeopleSoft Enterprise information to be used by the BI platform, the BI platform needs information on how to authenticate into your PeopleSoft Enterprise system.

9.6.2.1 To enable PeopleSoft Enterprise authentication in the BI platform

Procedure

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Double-click *PeopleSoft Enterprise*.
   The *PeopleSoft Enterprise* page appears. It has four tabs: *Options*, *Domains*, *Roles*, and *User Update*.
4. On the *Options* tab, select the *Enable PeopleSoft Enterprise Authentication* check box.
5. Make appropriate changes under *New Alias*, *Update Options*, and *New User Options* according to your BI platform deployment.

   Click *Update* to save your changes before proceeding to the *Domains* tab.
6. Click the *Domains* tab.
7. In the *PeopleSoft Enterprise System User* area, type a database User name and Password for the BI platform to use to log on to your PeopleSoft Enterprise database.
8. In the *PeopleSoft Enterprise Domains* area, enter the Domain name and QAS address used to connect to your PeopleSoft Enterprise environment, and click *Add*.

   > **Note**
   >
   > If you have multiple PeopleSoft domains, repeat this step for any additional domains you want to have access to. The first domain you enter will become the default domain.
9. Click *Update* to save your changes.

9.6.3 Mapping PeopleSoft roles to the BI Platform

The BI platform automatically creates a group for each PeopleSoft role that you map. As well, the program creates aliases to represent the members of the mapped PeopleSoft roles.

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in the BI platform.

Doing so reduces the number of accounts that are created for the same user in the BI platform.

For example, if you run PeopleSoft HR 8.3 and PeopleSoft Financials 8.4, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in the BI platform.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

For example, if you run PeopleSoft HR 8.3 with a user account for Russell Aquino (user name "raquino"), and you run PeopleSoft Financials 8.4 with a user account for Raoul Aquino (user name "raquino"), then you need to create a separate account for each user's alias. Otherwise, the two users are added to the same BI platform account; they will be able to log in to the BI platform with their own PeopleSoft credentials and have access to data from both PeopleSoft systems.

9.6.3.1 To map a PeopleSoft role to the BI Platform

Prerequisites

If the BI platform JVM (Java virtual machine) does not have a certificate to the PeopleSoft server, you will need to perform these additional steps before the main steps below:

1. Get the .cer file from the PeopleSoft server.
2. Copy the .cer file to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Execute the following command from the security directory: `"<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <peoplesoftserver>.cer -keystore cacerts -alias <peoplesoftserver>`.
4. Restart the web application server.

Context

Main steps:

Procedure

1. Log on as an administrator to the Central Management Console.
2. Click *Authentication*.
3. Double-click *PeopleSoft Enterprise*.
4. On the *Roles* tab, in the PeopleSoft Enterprise Domains area, select the domain associated with the role you want to map to the BI platform.
5. Use one of the following options to select the roles you want to map:
   - In the *PeopleSoft Enterprise Roles* area, in the Search roles box, enter the role you want to locate and map to the BI platform, and then click >.
   - From the *Available Roles* list, select the role you want to map to the BI platform and click >.

   > **Note**
   >
   > When searching for a particular user or role, you can use the wild card %. For example, to search for all roles beginning with "A," type *A%*. Search is also case sensitive.

   > **Note**
   >
   > If you want to map a role from another domain, you must select the new domain from the list of available domains to match a role from a different domain.
6. Go to the *User Update* tab and either click the *Update* button, or schedule the updates.
7. On the *Options* tab, go to the *New User Options* area and select one of the following options:
   - *Assign each added alias to an account with the same name*
     Select this option if you run multiple PeopleSoft Enterprise systems with users who have accounts on more than one system (and no two users have the same user name for different systems).
   - *Create a new account for every added alias*
     Select this option if you run only one PeopleSoft Enterprise, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.
8. In the *Alias Update Options* area, select one of the following options:
   - *Create new aliases when the Alias Update occurs*
     Select this option to create a new alias for every user that is mapped to the BI platform. New accounts are added for users without the BI platform accounts or for all users if you selected the Create a new account for every added alias option.
   - *Create new aliases only when the user logs on*
     Select this option if the role that you want to map contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to the BI platform for the first time. This is the default option.
9. In the *New User Options* area specify how new users are created.

   Select one of the following options:

   - *New users are created as named users.*
     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are

connected. You must have a named user license available for each user account created using this option.

> **Note**
>
> Number of concurrent logon sessions for a named user created using Named User license is limited to 10. If such a named user tries to log into the 11th concurrent logon session, the system displays an approprite error message. You need to release one of the existing sessions to be able to log in.
>
> However, there is no restriction on the number of concurrent logon sessions for named users created using Processor license and Public Document license.

- *New users are created as concurrent users.*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the BI platform, a 100 user concurrent license could support 250, 500, or 700 users.

The roles that you selected now appear as groups in the BI platform.

9.6.3.2 Remapping consideration

If you add users to a role that has already been mapped to the BI platform, you need to remap the role to add the users to the BI platform. When you remap the role, the option to map users as either named users or concurrent users affects only the new users that you added to the role.

For example, you first map a role to the BI platform with the "New users are created as *named* users" option selected. Later, you add users to the same role and remap the role with the "New users are created as *concurrent* users" option selected.

In this situation, only the new users in the role are mapped to the BI platform as concurrent users; the users that were already mapped remain named users. The same condition applies if you first map users as concurrent users, and then you change the settings to remap new users as named users.

9.6.3.3 To unmap a role

Procedure

1. Log on as an administrator to the Central Management Console.
2. Click *Authentication*.
3. Click *PeopleSoft Enterprise*.
4. Click *Roles.*
5. Select the role that you want to remove, and click <.
6. Click *Update*.

Members of the role will no longer be able to access the BI platform, unless they have other accounts or aliases.

> ⓘ Note
>
> You can also delete individual accounts or remove users from roles before you map them to the BI platform to prevent specific users from logging on.

9.6.4 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your BI platform user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and BI platform users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- Update roles only: using this option will update only the links between the currently mapped roles that have been imported in the BI platform. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in the BI platform for new user aliases added to the ERP system.

> ⓘ Note
>
> If you have not specified to automatically create user aliases for updates when you enabled authentication, no accounts will be created for new aliases.

9.6.4.1 To schedule user updates

Context

After you map roles into the BI platform, you need to specify how the system updates these roles.

Procedure

1. Click the *User Update* tab.
2. Click *Schedule* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

> → Tip
>
> If you want to run an update immediately click *Update Now*.

> → Tip
>
> Use the *Update Roles Only* option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

The *Recurrence* dialog box appears.

3. Select an option from the *Run Object* list and provide all the requested scheduling information.

   When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule* after you have finished providing the scheduling information.
   The date of the next scheduled role update is displayed in the *User Update* tab.

> ⓘ Note
>
> You can always cancel the next scheduled update by clicking *Cancel Scheduled Updates* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

9.6.5 Using the PeopleSoft Security Bridge

The Security Bridge feature of the BI platform allows you to import PeopleSoft EPM security settings to the BI platform.

The Security Bridge operates in two modes:

- **Configuration mode**
  In configuration mode, the Security Bridge provides an interface that enables you to create a response file. This response file is what governs the behavior of the Security Bridge during execution mode.
- **Execution mode**
  Based on the parameters that you define in the response file, the Security Bridge imports the security settings of dimension tables in PeopleSoft EPM to universes in the BI platform.

9.6.5.1 Importing security settings

To import the security settings, you must do the following tasks in order:

- Define the objects that the Security Bridge will manage.
- Create a response file.
- Run the Security Bridge application.

For information about managing security after you import the settings, see Managing security settings [page 365].

9.6.5.1.1 Defining managed objects

Before you run the Security Bridge, it is important to determine the objects that are managed by the application. The Security Bridge manages one or more PeopleSoft roles, a BI platform group, and one or more universes.

- Managed PeopleSoft roles
  These are roles in your PeopleSoft system. Members of these roles work with PeopleSoft data through PeopleSoft EPM. You must choose the roles that include the members for whom you want to provide/update access privileges to the managed universes in the BI platform.
  The access rights that are defined for the members of these roles are based on their rights in PeopleSoft EPM; the Security Bridge imports these security settings to the BI platform.
- Managed BI platform group
  When you run the Security Bridge, the program creates a user in the BI platform for each member of a managed PeopleSoft role.
  The group in which the users are created is the managed BI platform group. Members of this group are the users whose access rights to the managed universes are maintained by the Security Bridge. Because the users are created in one group, you can configure the Security Bridge not to update the security settings for certain users simply by removing users from the managed BI platform group.
  Before you run the Security Bridge, you must choose a group in the BI platform to be the location where the users are created. If you specify a group that does not exist, the Security Bridge will create the group in the BI platform.
- Managed universes
  Managed universes are the universes to which the Security Bridge imports security settings from PeopleSoft EPM. From the universes that are stored in your BI platform system, you must choose which ones are to be managed by the Security Bridge. Members of managed PeopleSoft roles who are also members of the managed BI platform group cannot access any data through these universes that they cannot access from PeopleSoft EPM.

9.6.5.1.2 To create a response file

Procedure

1. Go to the folder that you specified during the installation of the Security Bridge, and run the `crpsepmsecuritybridge.bat` (in Windows) and `crpsepmsecuritybridge.sh` (in Unix) file.

   > **Note**
   >
   > In Windows, by default, this location is `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`.

   The Security Bridge for PeopleSoft EPM dialog box appears.
2. Select *New* to create a response file, or select *Open* and click *Browse* to specify a response file that you want to modify. Select the language you want for the file.
3. Click *Next*.
4. Provide the locations of the *PeopleSoft EPM SDK* and the *BI Platform SDK*.

   > **Note**
   >
   > The PeopleSoft EPM SDK is typically located on the PeopleSoft server at `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.

   > **Note**
   >
   > The BI platform SDK is typically located at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`.
5. Click *Next*.

   The dialog box prompts you for connection and driver information for the PeopleSoft database.
6. From the Database list, select the appropriate database type, and provide the information for the following fields:

Field	Description
Database	The name of the PeopleSoft database.
Host	The name of the server that hosts the database.
Port number	The port number for accessing the server.
Class location	The location of the class files for the database driver.
User name	Your user name.
Password	Your password.

7. Click *Next*.

   The dialog box displays a list of all the classes that the Security Bridge will use to run. If necessary, you can add to or remove classes from the list.
8. Click *Next*.

   The dialog box prompts you for connection information for the BI platform.

9. Provide the appropriate information for the following fields:

Field	Description
Server	The name of the server where the Central Management Server (CMS) is located.
User name	Your user name.
Password	Your password.
Authentication	Your authentication type.

10. Click *Next*.
11. Choose a BI platform group, and click *Next*.

> **Note**
>
> The group that you specify in this field is where the Security Bridge creates users for the members of the managed PeopleSoft roles.

> **Note**
>
> If you specify a group that does not already exist, it will be created by the Security Bridge.

The dialog box displays a list of roles from your PeopleSoft system.

12. Select the *Imported* option for the roles that you want the Security Bridge to manage, and click *Next*.

> **Note**
>
> The Security Bridge creates a user in the managed BI platform group (which you specified in the previous step) for each member of the role(s) that you select.

The dialog box displays a list of universes in the BI platform.

13. Select the universe(s) to which you want the Security Bridge to import security settings, and click *Next*.
14. Specify a filename for the Security Bridge log file and a location where the log file will be saved. You can use the log file to determine whether or not the Security Bridge is successful in importing the security settings from PeopleSoft EPM.
15. Click *Next*.

    The dialog box displays a preview of the response file that the Security Bridge will use during execution mode.
16. Click *Save*, and choose a location where you want to save the response file.
17. Click *Next*.

    You have successfully created the response file for the Security Bridge.
18. Click *Exit*.

> **Note**
>
> The response file is a Java property file that you can also create and/or modify manually. For more details, see the “PeopleSoft response file” section.

9.6.5.2 Applying the security settings

To apply the security settings, run the `crpsepmsecuritybridge.bat` batch file (on Windows) or the `crpsempsecuritybridge.sh` file (on Unix), and use the response file that you created as an argument. For example, type **`crpsepmsecuritybridge.bat myresponsefile.properties`** on Windows, or **`crpsempsecuritybridge.sh myresponsefile.properties`** on Unix.

The Security Bridge application runs. It creates users in the BI platform for the members of the PeopleSoft roles that you specified in the response file and imports the security settings from PeopleSoft EPM to the appropriate universes.

9.6.5.2.1 Mapping considerations

During execution mode, the Security Bridge creates a user in the BI platform for each member of a managed PeopleSoft role.

The users are created to have only Enterprise authentication aliases, and the BI platform assigns random passwords to these users. As a result, the users cannot log on to the BI platform until the administrator manually reassigns new passwords or maps the role(s) to the BI platform through the PeopleSoft Security Plug-in to allow the users to log on by using their PeopleSoft credentials.

9.6.5.3 Managing security settings

You can manage the security settings that you applied by modifying the objects that are managed by the Security Bridge.

9.6.5.3.1 Managed users

The Security Bridge manages users based on the following criteria:

- Whether or not the user is a member of a managed PeopleSoft role.
- Whether or not the user is a member of the managed BI platform group.

If you want to enable a user to access PeopleSoft data through universes in the BI platform, ensure that the user is a member of *both* a managed PeopleSoft role and the managed BI platform group.

- For members of managed PeopleSoft roles who do not have accounts in the BI platform, the Security Bridge creates accounts and assigns random passwords to them. The administrator must decide whether or not to reassign new passwords manually or map the roles to the BI platform through the PeopleSoft Security Plug-in to allow the users to log on to the BI platform.
- For members of managed PeopleSoft roles who are also members of the managed BI platform group, the Security Bridge updates the security settings that are applied to the users so that they have access to the appropriate data from the managed universes.

If a member of a managed PeopleSoft role has an existing account in the BI platform, but he or she is *not* a member of the managed BI platform group, then the Security Bridge *does not* update the security settings that are applied to the user. Typically, this situation occurs only when the administrator manually removes user accounts that have been created by the Security Bridge from the managed BI platform group.

> ⓘ Note
>
> This is an effective method for managing security: by removing users from the managed BI platform group, you can configure their security settings to be different from the security settings that they have in PeopleSoft.

Conversely, if a member of the managed BI platform group is *not* a member of a managed PeopleSoft role, then the Security Bridge *does not* provide them with access to the managed universes. Typically, this situation occurs only when PeopleSoft administrators remove users who have been previously mapped to the BI platform by the Security Bridge from the managed PeopleSoft role(s).

> ⓘ Note
>
> This is another method for managing security: by removing users from managed PeopleSoft roles, you can ensure that the users have no access to data from PeopleSoft.

9.6.5.3.2 Managed universes

The Security Bridge manages universes through restriction sets, which limit the data that managed users can access from the managed universes.

Restriction sets are groups of restrictions (for example, restrictions to Query Controls, SQL Generation, and so on). The Security Bridge applies/updates Row Access and Object Access restrictions for the managed universes:

- It applies Row Access restrictions to dimension tables that are defined in PeopleSoft EPM. These restrictions are user-specific and can be configured to one of the following settings:
  - The user has access to all of the data.
  - The user has access to none of the data.
  - The user has access to data based on their row-level permissions in PeopleSoft, which are exposed through the Security Join Tables (SJT) that are defined in PeopleSoft EPM.
- It applies Object Access restrictions to measure objects based on the fields that are accessed by the measure objects.
  If a measure object accesses fields that are defined as metrics in PeopleSoft, then access to the measure object is allowed/disallowed depending on whether or not the user can access the referenced metrics in PeopleSoft. If a user cannot access any of the metrics, then access to the measure object is denied. If the user can access all of the metrics, then access to the measure object is granted.

As an administrator, you can also limit the data that users can access from your PeopleSoft system by limiting the number of universes that are managed by the Security Bridge.

9.6.5.4 PeopleSoft response file

The Security Bridge feature of the BI platform operates based on the settings that you specify in a response file.

Typically, you generate the response file by using the interface that is provided by the Security Bridge in configuration mode. However, because the file is a Java property file, you can also create or modify it manually.

This appendix provides information about the parameters that you need to include in the response file if you choose to generate it manually.

> ⓘ Note
>
> When you create the file, you must respect the Java property file escaping requirement (for example, ':' is escaped as '\:').

9.6.5.4.1 Response file parameters

The following table describes the parameters that are included in the response file:

Parameter	Description
classpath	The class path for loading the necessary .jar files. Multiple class paths must be separated by a ';' on both Windows and UNIX. The class paths that are needed are for the `com.peoplesoft.epm.pf.jar` and the JDBC driver .jar files.
db.driver.name	The JDBC driver name that is used to connect to the PeopleSoft database (for example, `com.microsoft.jdbc.sqlserver.SQLServerDriver`).
db.connect.str	The JDBC connection string that is used to connect to the PeopleSoft database (for example, `jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO`)
db.user.name	The user name for logging on to the PeopleSoft database.
db.password	The password for logging on to the PeopleSoft database.
db.password.encrypted	The value for this parameter determines whether the password parameter in the response file is encrypted or not. The value can be set to either True or False. (If no value is specified, the value becomes False by default.)

Parameter	Description
enterprise.cms.name	The CMS in which the universes are located.
enterprise.user.name	The user name for logging on to the CMS.
enterprise.password	The password for logging on to the CMS.
enterprise.password.encrypted	The value for this parameter determines whether the password parameter in the response file is encrypted or not. The value can be set to either True or False. (If no value is specified, the value becomes False by default.)
enterprise.authMethod	The authentication method for logging on to the CMS.
enterprise.role	The managed BI platform group. For more information, see Defining managed objects [page 362].
enterprise.license	Controls the license type when importing users from PeopleSoft. "0" sets the named user license, "1" sets the concurrent user license.
peoplesoft.role.n	The list of managed PeopleSoft roles. For more information, see Defining managed objects [page 362]. **<n>** is an integer, and each entry occupies a property with the peoplesoft.role prefix. **Note** **<n>** is 1 based. You can use '*' to denote all available PeopleSoft roles, given that n is 1, and it is the only property that has peoplesoft.role as the prefix in the response file.
mapped.universe.n	The list of universes that you want the Security Bridge to update. For more information, see Defining managed objects [page 362]. **<n>** is an integer, and each entry occupies a property with the mapped.universe prefix. **Note** **<n>** is 1 based. You can use '*' to denote all available universes, given that n is 1, and it is the only property that has mapped.universe as the prefix in the response file.
log4j.appender.file.File	The log file that is written by the Security Bridge.

Parameter	Description
log4j.*	Default log4j properties that are required for log4j to function properly: log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n
peoplesoft classpath	The class path to the PeopleSoft EPM API .jar files. This parameter is optional.
enterprise.classpath	The class path to the BI platform SDK .jar files. This parameter is optional.
db.driver.type	The PeopleSoft database type. This parameter can have one of the following values: Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Custom Custom may be used to specify databases other than the recognized types or versions. This parameter is optional.
sql.db.class.location sql.db.host sql.db.port sql.db.database	The location of the SQL Server JDB driver .jar files, the SQL Server host machine, the SQL Server port, and the SQL Server database name. These parameter can be used only if the db.driver.type is Microsoft SQL Server 2000. These parameters are optional.

Parameter	Description
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	The location of the Oracle JDBC driver .jar files, the Oracle database host machine, the Oracle database port, and the Oracle database SID. These parameters can be used only if the db.driver.type is Oracle Database 10.1. These parameters are optional.
db2.db.class.location db2.db.host db2.db.port db2.db.sid	The location of the DB2 JDBC driver .jar files, the DB2 database host machine, the DB2 database port, and the DB2 database SID. These parameters can be used only if the db.driver.type is DB2 UDB 8.2 Fixpack 7 These parameters are optional.
custom.db.class.location custom.db.drivername custom.db.connectStr	The location, name, and connection string of the custom JDBC driver. These parameters can be used only if the db.driver.type is Custom. These parameters are optional.

9.7 X.509 Authentication

9.7.1 X.509 Authentication for BI Launch Pad

9.7.1.1 Creating and Configuring Certificates and Keystores

Context

> ⓘ Note
>
> A user should exist in the BI platform to achieve Single Sign-On through X.509 authentication.

> ⓘ Note
>
> Download and install OpenSSL toolkit to perform the steps below.

> **Note**
>
> Follow all the steps below if you have to create a CA certificate and self-sign it.

> **Note**
>
> If you have a trusted CA, refer to With Trusted CA [page 372] for creating and configuring certificates and keystores.

Procedure

1. Run the command to create Certificate Authority (CA) key (ca.key) and certificate request (ca.csr) files. `Openssl.exe req –newkey rsa:2048 –nodes –out c:\ssl\ca.csr –keyout c:\ssl\ca.key`
2. Run the command to create a signed certificate ca.pem. `Openssl.exe x509 –req –trustout –signkey c:\ssl\ca.key –days 365 –in c:\ssl\ca.csr –out c:\ssl\ca.pem`
3. Create the server key-pair, certificate, and keystore.
   a. Create a file to hold the CA's serial numbers by running the code: `Echo 02 >c:\ssl\ca.srl`
   b. Go to `C:\Program Files\Java\jre7\bin` and use keytool.exe to create server keystore, certificate, and private key.

      > **Note**
      >
      > In the location of Java keytool.exe, 'jre7' might vary depending on the version of Java.

      ```
      Keytool.exe –genkey –alias server –keyalg RSA –keysize 2048 –keystore c:\ssl\serverkeystore.jks –storetype JKS
      Keytool.exe –certreq –keyalg RSA –alias server –file c:\ssl\server.csr –keystore c:\ssl\serverkeystore.jks
      ```

      > **→ Remember**
      >
      > While generating the certificate, enter the hostname of the server machine when prompted. Otherwise you will get a certificate error on the client when connecting.

   c. Enter the keystore password.

      > **→ Remember**
      >
      > You need to edit the request file server.csr in a text editor, and change "New Begin Certificate Request" to "Begin Certificate Request" and "New End Certificate Request" to "End Certificate Request".
4. Run the command to create the signed certificate - server.crt. `Openssl.exe x509 –CA c:\ssl\ca.pem –cakey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\server.csr –out c:\ssl\server.crt –days 365`
5. Import the certificate authority and server certificate into the server keystore.

   ```
   Keytool.exe –import –alias ca –keystore c:\ssl\serverkeystore.jks –trustcacerts –file c:\ssl\ca.pem
   ```

```
Keytool.exe –import –alias server –keystore c:\ssl\serverkeystore.jks –
trustcacerts –file c:\ssl\server.crt
```

6. Run the command to create the client certificates, client.req and client.key. `Openssl.exe –newkey rsa:2048 –nodes –out c:\ssl\client.req –keyout c:\ssl\client.key –config c:\ssl\sslc.cnf`

> **Note**
>
> Copy sslc.cnf file from the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` to C:\SSL and change the parameters:
>
> Dir=c:/ssl # location for everything
>
> Certificate= $dir/ca.pem # CA certificate
>
> Private_key= $dir/ca.key # private key
>
> RANDFILE= $dir/.rand # private random number file

7. Run the command to sign the client certificate. `Openssl.exe x509 –CA c:\ssl\ca.pem –CAkey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\client.req –out c:\ssl\client.pem –days 365`
8. Import the CA and client certificate into the trust keystore using the command below. The command creates trustkeystore.jks.

```
Keytool.exe –import –alias ca –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\ca.pem
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

9. Export the client certificate with the client private key PKCS12 format. `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. The command creates the client.p12 file.
10. Run the command to export CA certificate and create ca.crt. `Openssl.exe x509 –in c:\ssl\ca.pem –inform PEM –out c:\ssl\ca.crt –outform DER`
11. Copy the .p12 and ca.crt files to the client machine to install the client and CA certificate.

> **Note**
>
> For installing certificates in Mozilla Firefox, go to *Tools* > *Options* > *Advanced* and select View Certificates in the Encryption tab to import the client.p12 file under the Your Certificates tab and ca.crt file under the Authorities tab.

9.7.1.1.1 With Trusted CA

Context

Procedure

1. Create the server key-pair, certificate, and keystore.
   a. Create a file to store the CA's serial numbers by running the code: `Echo 02 >c:\ssl\ca.srl`
   b. Go to `C:\Program Files\Java\jre7\bin` and use keytool.exe to create the server keystore, certificate, and private key.

      > **Note**
      >
      > In the location of keytool.exe, 'jre7' might vary depending on the version of Java.

      ```
      Keytool.exe –genkey –alias server –keyalg RSA –keysize 2048 –keystore
      c:\ssl\serverkeystore.jks –storetype JKS
      Keytool.exe –certreq –keyalg RSA –alias server –file c:\ssl\server.csr –
      keystore c:\ssl\serverkeystore.jks
      ```

      > **→ Remember**
      >
      > When generating the certificate, enter the hostname of the server machine when prompted. Otherwise you will get a certificate error on the client when connecting.

   c. Enter the keystore password.

      > **→ Remember**
      >
      > You need to edit the request file server.csr in a text editor, and change "New Begin Certificate Request" to "Begin Certificate Request" and "New End Certificate Request" to "End Certificate Request".

2. Run the command to create the signed certificate - server.crt. `Openssl.exe x509 –CA c:\ssl\ca.pem –cakey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\server.csr –out c:\ssl\server.crt –days 365`
3. Import server certificate into the server keystore.

   ```
   Keytool.exe –import –alias server –keystore c:\ssl\serverkeystore.jks –
   trustcacerts –file c:\ssl\server.crt
   ```

4. Run the command to create client certificates, client.req and client.key. `Openssl.exe –newkey rsa:2048 –nodes –out c:\ssl\client.req –keyout c:\ssl\client.key –config c:\ssl\sslc.cnf`

   > **Note**
   >
   > Copy the sslc.cnf file from the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` to C:\SSL and change the parameters:
   >
   > Dir=c:/ssl # location for everything
   >
   > Certificate= $dir/ca.pem # CA certificate
   >
   > Private_key= $dir/ca.key # private key
   >
   > RANDFILE= $dir/.rand # private random number file

5. Run the command to sign the client certificate. `Openssl.exe x509 –CA c:\ssl\ca.pem –CAkey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\client.req –out c:\ssl\client.pem –days 365`
6. Import the client certificate into trust keystore with the command given below. The command creates trustkeystore.jks.

```
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –trustcacerts –file c:\ssl\client.pem
```

7. Export the client certificate with the client private key PKCS12 format. `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. The command creates the client.p12 file.
8. Copy the .p12 file to the client machine to install it.

> **Note**
>
> For installing certificates in Mozilla Firefox, go to *Tools* > *Options* > *Advanced* and select View Certificates in the Encryption tab to import the client.p12 file under the Your Certificates tab and ca.crt file under the Authorities tab.

9.7.1.2 Configuring Tomcat SSL Server

9.7.1.2.1 One-Way SSL Configuration

Procedure

1. Go to `<INSTALLDIR>\tomcat\conf\server.xml`
2. Edit the xml tag: `<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true"> <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>`

> **Note**
>
> The password (Password1) and location (C:\ssl\serverkeystore.jks) of the keystore file used in the xml tag above are just examples. You can use any password and location of your choice.

3. Save the file and restart the Tomcat server.

9.7.1.2.2 Two-Way SSL Configuration

Context

Configure the Tomcat server to request client authentication by following the steps below.

Procedure

1. Go to `<INSTALLDIR>\tomcat\conf\server.xml`
2. Edit server.xml with the xml tag given below:
   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
   <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
   myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
   Connector>
   ```

   > **Note**
   >
   > The password (Password1) and location (C:\ssl\serverkeystore.jks or C:\ssl\trustkeystore.jks) of the server keystore and trust keystore file used in the xml tag above are just examples. You can use any password and location of your choice.

3. Save the file and restart the Tomcat server.

   > **Note**
   >
   > In Internet Explorer, disable the option "Don't prompt for client certificate selection when no certificates or only one certificates or only one certificates exist" by navigating to *Internet Options* > *Security* > *Local Internet* > *Custom Level* > *Miscellaneous*.

9.7.1.3 Configuring BI Launch Pad

9.7.1.3.1 Recreating a shared secret key

The shared secret key is used to establish trust between the client and the CMS. You need to configure the server before the client for Trusted Authentication.

Procedure

1. Login to the CMC.
2. Navigate to Authentication and select Enterprise.
3. Enable Trusted Authentication.
4. Select New Shared Secret.

   > **Note**
   >
   > The shared secret key is generated and the download message appears.

5. Select Download Shared Secret.
6. Select Save in the download dialog box and choose one of the following directories:
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

9.7.1.3.2 Passing the Shared Secret Key via the TrustedPrincipal.conf File

Procedure

1. Create a new text file in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEBINF\config\custom\directory`.
2. In the new file, add the text given below.

```
sso.enabled=true
        trusted.auth.user.retrieval=WEB_SESSION
        trusted.auth.user.param=MyUser
        trusted.auth.shared.secret=MySecret
```

3. Save the file and name it 'global.properties'.

9.7.1.3.3 Editing the custom.jsp File

Context

> **Note**
>
> Create a user with machine name in CMC before editing the custom.jsp file.

Procedure

1. Go to
   a. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* in *com.businessobjects.webpath.InfoView.jar* for classic BI Launch Pad.
   b. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* in *com.businessobjects.webpath.fioriBI.jar* for Fiorified BI Launch Pad.
2. Edit the custom.jsp file.

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code
request.getSession().setAttribute("MySecret","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Note**
>
> You should replace the <Shared_Secret_Key> with the new key available in the *TrustedPrincipal.conf* file. See Recreating a shared secret key [page 376] to learn how to create a shared secret key.

9.7.1.3.4 Creating the myScript.js File

Context

Procedure

1. Go to *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* and create myScript.js.
2. Add the following to myScript.js:

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Restart the Tomcat server.

9.7.1.3.5 Setting Up the BOE Internal and Custom Property Files

Procedure

1. Navigate to *<INSTALLDIR>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal*
2. Open the bilaunchpad.properties file and change the following properties:

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Restart the Tomcat server.

9.7.1.3.6 Setting Up the BOE Web.xml Files

Procedure

1. Go to `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`
2. Edit the web.xml file in this location with the code shown below:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbridge.customconfig,com.businessobjects.servletbridge.external,com.businessobjects.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.siebel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-value>
</init-param>
```

3. Add the parameters to the web.xml file by following the steps below:
   a. `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`
   b. Add the parameters below:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. Repeat the steps by navigating to `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`

> → Tip
>
> To verify that you have properly configured trusted authentication, use the following URL to access the BI launch pad application: https://[cmsname]:8443/BOE/BI/logon.jsp, where [cmsname] is the name of the machine hosting the CMS.

9.7.2 X.509 Authentication for Web Services

9.7.2.1 For SOAP Web Services

9.7.2.1.1 Configuring SSL in Tomcat

Context

When using web services, you need to configure SSL in Tomcat before configuring the SAP Business Intelligence platform.

> **Note**
>
> A user should exist in the BI platform to achieve Single Sign-On through X.509 authentication.

Procedure

1. Go to `<INSTALLDIR>\tomcat\conf`.
2. Open server.xml in an XML editor and edit the xml tag:

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
   <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
   myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
   Connector>
   ```
3. Save the file.

> **Note**
>
> The password and location of the files mentioned above are just examples. You can add any password and location of your choice.

> **Note**
>
> You can refer to Creating and Configuring Certificates and Keystores [page 370] for more information on creating and configuring keystore files.

9.7.2.1.2 Configuring the axis2.xml File

Context

> **Note**
>
> In Linux or Unix, ensure that the OS BI install user has recursive 755 rights on the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje` before performing the steps below. The rights can be assigned by using the command `chmod -R 755`

Procedure

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
2. Open axis2.xml file in any XML editor.
3. Update the xml tag with new port number to allow a secured connection.

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> **Note**
>
> The default configuration assumes that AxisServlet only receives requests through http. To allow https, you need to configure AxisServletListener with the name = "https" and specify the port parameter on both receivers. In addition, you can add or remove multiple port numbers by updating the xml tags.

4. Save axis2.xml.
5. Restart the Tomcat server.
6. Launch any browser and go to https://<IP address>:<https port>/dswsbobje/services/listServices to validate the secure connection. After you navigate to the link, trustedLoginWithX509 is displayed under the Session tab.

9.7.2.1.3 Regenerating a shared secret value

Context

You can regenerate a new secret using the legacy method for configuring trusted authentication.

Procedure

1. Launch Central Management Console.
2. Go to *Authentication* > *Enterprise.*
3. Under *Trusted Authentication*, check the box against *Trusted Authentication is enabled*.
4. Choose *New Shared Secret*. This will generate the shared secret key.
5. Choose *Download Shared Secret* and then *Update*.
6. Copy the downloaded file TrustedPrincipal.conf to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` in Windows.

> **Note**
>
> You can view the shared secret value by opening TrustedPrincipal.conf in any XML editor.

9.7.2.1.4 Configuring web.xml File

Context

Procedure

1. Go to `<INSTALLDIR>\tomcat\webapps\dswsbobje\WEB-INF.`
2. Open web.xml in an XML editor and update the xml tag with the CMS host machine name:

```
<context-param>
        <param-name>cms.default</param-name>
        <param-value>EnterHostMachineName</param-value>
    </context-param>
```

3. Add the xml tag below with the shared secret value. For more information on how to generate a shared secret value, refer to Regenerating a shared secret value [page 382].

```
<context-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>shared secret value</param-value>
</context-param>
```

4. Save the web.xml file.

> **Note**
>
> The configurations made in the axis2.xml file will be discarded if you upgrade from a version lower than BI 4.2 SP04.

9.7.2.2 For RESTful Web Services

> **Note**
>
> A user should exist in the BI platform to achieve single sign-on through X.509 authentication.

Check the topic Configuring HTTPS/SSL in *Business Intelligence platform Administrator Guide* to establish trusted authentication for RESTful web services.

To establish Trusted Authentication using X.509 certificates, you must generate a shared secret key. If you are using the legacy method, see Regenerating a shared secret value [page 382] in the *Business Intelligence Platform CMC Help Guide*. If you are using the new method, see Configure the server to use Trusted Authentication in the *Business Intelligence platform Administrator Guide* for more information.

In addition, for more details on the REST SDK endpoint, refer to `API Reference Authentication /v1//logon/trustedx509` in *Business Intelligence platform RESTful Web Service Developer Guide*.

9.7.2.2.1 X.509 Authentication for RESTful Web Services on Tomcat

Context

In public key cryptography, X.509 is a standard that defines the requirements for a secure digital certificate. An X.509 certificate verifies the possession of the public key by a user or a services identity.

You can now enable X.509 authentication for RESTful web services on Tomcat application server by following the steps below:

Procedure

1. Enable SSL on Tomcat. Refer to Configuring SSL in Tomcat [page 380] for more information.
2. Generate a shared secret key. Refer to Regenerating a shared secret value [page 382] for more information.
3. Open the shared secret key file in a text editor.
4. Copy the shared secret key.
5. Edit the *biprws.properties* file.
   a. Go to `<INSTALLDIR>/tomcat/webapps/biprws/WEB-INF/config/default`.
   b. Open the *biprws.properties* file in a text editor.
   c. Search for *Trusted_Auth_Shared_Secret=*.
   d. Paste the shared secret key against the value *Trusted_Auth_Shared_Secret=*.
   e. Save the *biprws.properties* file.

9.7.3 X.509 Authentication for CMC

> **Note**
>
> A user should exist in the BI platform to achieve Single Sign-On through X.509 authentication.

You can achieve single sign-on through X.509 authentication by following these steps:

1. Creating and Configuring Certificates and Keystores [page 370]
2. One-Way SSL Configuration [page 374]
3. Two-Way SSL Configuration [page 375]
4. Recreating a shared secret key [page 376]
5. Passing the Shared Secret Key via the TrustedPrincipal.conf File [page 376]
6. Editing the Custom.jsp File (For CMC) [page 385]
7. Creating the myScript.js File (For CMC) [page 386]
8. Setting Up the BOE Internal and Custom Property Files (For CMC) [page 386]
9. Setting Up the BOE Web.xml File (For CMC) [page 386]

9.7.3.1 Editing the Custom.jsp File (For CMC)

Context

> **Note**
>
> Create a user with machine name in CMC before editing the custom.jsp file. In a machine, if a user exists, you can proceed directly with the below steps.

Procedure

1. Go to `<INSTALLDIR>\tomcat\webapps\BOE\WEBINF\eclipse\plugins\webpath.CmcApp\web\cutom.jsp` in com.businessobjects.webpath.InfoView.jar.
2. Edit the custom.jsp file

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code request.getSession().setAttribute("MySecret","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Note**
>
> You should replace the shared secret value in this code with the new key and the user with the machine name created in CMC.

9.7.3.2 Creating the myScript.js File (For CMC)

Procedure

1. Go to `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\noCacheCustomResources and create myScript.js`.
2. Add the following to myScript.js:

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Restart the Tomcat server.

9.7.3.3 Setting Up the BOE Internal and Custom Property Files (For CMC)

Procedure

1. Navigate to `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\internal\CmcApp.properties`.
2. Open the CmcApp.properties file and add the parameters:

   ```
   sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter,
   trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela,
   trustedX509, sapSSO, sitemindera
   ```

3. Restart the Tomcat server.

9.7.3.4 Setting Up the BOE Web.xml File (For CMC)

Procedure

1. Go to `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.

2. Edit the web.xml file in this location with the code shown below:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbridge.customconfig,com.businessobjects.servletbridge.external,com.businessobjects.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.siebel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-value>
</init-param>
```

3. Add the parameters to the web.xml file by following the steps below:
   a. Go to `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`
   b. Add the parameters below:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>Shared_Secret_Key</param-value>
</init-param>
```

   c. Repeat the steps by navigating to `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`

> **Note**
>
> To verify that you have properly configured trusted authentication, use the following URL to access the BI launch pad application: https://[cmsname]:8443/BOE/BI/logon.jsp, where [cmsname] is the name of the machine hosting the CMS.

9.8 OpenID Connect authentication

You can enable OpenID Connect authentication.

OpenID Connect authentication works based on authentication server (OAuth). Like for the cloud drive support, OpenID Connect authentication also relies on authentication server configuration. For more information on authentication server configuration, see Authorization Server Configuration [page 672].

OpenID Connect authentication is developed on top of Enterprise authentication.

Like in the case of SAML authentication, users must be imported to the BI Platform in advance as Enterprise users (secEnterprise).

> **Note**
>
> While importing users, you need to ensure that the email ID of the user is also included.

Unlike SAML authentication, the following applies for OpenID Connect authentication:

- All the configurations should be done in the BI Platform backend, not at the application server layer.
- It does not depend on trusted authentication.

OpenID Connect authentication is only supported for BI Launch Pad and OpenDocument.

9.8.1 Enabling OpenID Connect authentication

OpenID Connect authentication is only supported for BI Launch Pad and OpenDocument.

For information on how to enable OpenID Connect authentication, see Enterprise authentication settings [page 231]. After enabling the OpenID Connection authentication at the Enterprise authentication plugin in the backend, you need to enable the same application layer for the supported applications (for example, `FioriBI.properties` file for the BI Launch Pad and the `OpenDocument.properties` file for the OpenDocument applications under `WEB-INF/config/custom`.

To enable the web SSO authentication workflow, set `logon.webssoauthentication.framework` to `OpenId`.

Set `openid.restful.url` to the RESTful web services URL of the landscape (for example, `https://<server>:8443/biprws`).

You can log in to the BI Launch Pad through OpenID using the `.../BO/BI` URL. However, once you log in using the OpenID Connect authentication to BI Launch Pad, you can observe that a placeholder context path "WEBSSO" will be added to the URL. This will stay on the URL path even after logging out. If you want to log in again from the same window using the same URL, you will need to remove "WEBSSO" from the browser URL.

10 Data Source Reference

10.1 Enhanced Credential Mapping

In BI 4.2.X and earlier releases, an administrator could save only one set of database credentials for every user in CMC.

This functionality requires the administrator to maintain the same credentials for all their different databases. From BI 4.3 onwards, you can save multiple sets of database credentials for each user through data source references.

> ⓘ Note
>
> The Enhanced Credential Mapping feature introduced in SAP BusinessObjects Business Intelligence Platform 4.3 is only supported in Information Design Tool.

Data source reference in CMC

In CMC, an administrator creates a data source reference in the BI platform. This data source reference is then used in the user properties where the administrator defines one set of the database credentials against it. This data source reference is then used as part of Credential Mapping, which is a mode of authentication available in the Connections.

The administrator gets an option to select the data source reference of their choice when Credential Mapping is selected as the mode of authentication. In a similar way, an administrator can create multiple data source references if they've multiple databases connecting to the BI platform and define unique credentials for each user.

> ⓘ Note
>
> When you import users through a CSV file, promote users using Promotion Management tool, or when you select to synchronize the data source credentials during logon for Enterprise, LDAP, Windows AD authentication types, then the BI platform assigns the database credentials to the default data source reference.

Data source reference in BI Launch Pad

Data source referencing is also available in BI Launch Pad as well where you can update and map your user credentials.

> **Note**
>
> You cannot edit the *Data source reference* details, but you can edit the *Account Name*, *Password*, and *Confirm Password* fields.

How does it work?

Let's assume:

- That two data source references are available in the BI platform, for example, DSR1 for your sales database and DSR2 for your finance database
- Each data source reference has database credentials defined in the user properties of User A
- There are two connections CN1 and CN2 that are configured to use Credential Mapping as the mode of authentication
- DSR1 is associated with the connection CN1 and similarly DSR2 is associated with CN2

Now, if a User A tries to refresh a report that requires access to the sales database, then the BI platform looks for the DSR1 in the user properties and consumes the database credentials defined against DSR1 to establish a connection.

To use a data source reference, you've to complete the following tasks.

1. Create a data source reference [page 390]
2. Define the database credentials against a data source reference for a user in CMC [page 391]
3. Associate data source reference in OLAP connection [page 394]

> **Note**
>
> It is also possible to configure Credential Mapping for Relational Connections and OLAP Connections in Information Design Tool.

10.1.1 Create a data source reference

Context

A data source reference acts a variable that an administrator creates in the BI platform to save unique set of database credentials for each user. Follow the steps below to create a data source reference.

Procedure

1. Log in to CMC.
2. Under Define, go to Data Source References.
3. Select the icon (Create new data source reference).
4. Add the title of your data source reference and a description.
5. Select OK.

Results

You've successfully created a data source reference.

10.1.2 Define the database credentials against a data source reference for a user in CMC

Context

A data source reference should have a database credential defined in the user properties to allow the user to connect to a database. Follow the steps below to define the database credentials in CMC.

Procedure

1. Log in to CMC.
2. Go to *Users and Groups*.
3. Open the context menu of a user from the *User List*.
4. Go to *Properties* and select *Add* under *Data Source Credentials*.
5. Select the preferred data source reference.
6. Enter the values for *Account Name*, *Password*, and *Confirm Password*.
7. Repeat the process from Step 4 to add another data source reference.
8. Select *Save & Close*.

   You've successfully defined the database credentials for a data source reference.

10.1.3 Define the database credentials against a data source reference for a user in BI Launch Pad

Context

A data source reference should have a database credential defined in the user properties to allow the user to connect to a database.

Data source referencing is now available in BI Launch Pad as well, where you can update and map your user credentials. The database credentials is synced between CMC and BI Launch Pad.

Follow the steps below to define the database credentials in BI Launch Pad.

Procedure

1. Log in to BI Launch Pad.
2. Go to (User Settings), click the (*Settings*) option from the dropdown.

   The *Settings* window is displayed.
3. Click *User Account (Administrator)*.

   The User Account page opens with two tabs: *Account Information*, *Database Credentials*, and *Authorization Tokens*.
4. Click *Database Credentials*.

   You can view the synced data of the user from CMC displayed here.

   > **Note**
   >
   > You cannot edit the *Data source reference* details.
   >
   > But you can edit the *Account Name*, *Password*, and *Confirm Password* fields.

   When you change your password, a toast message is displayed on the screen *Changes to some preferences will take effect after the page reloads*.
5. Click *Save* and *Close* to save the mapped credential changes.

10.1.4 Define the database credentials against a data source reference for a group

Context

A data source reference should have a database credential defined in the user properties to allow the user to connect to a database.

> **Note**
>
> This task doesn't update the data source references for the members of the sub-groups. You can follow the same steps for the sub-group to update the data source references for its members.

Follow the steps below to define the database credentials:

Procedure

1. Log in to CMC.
2. Go to *Users and Groups*.
3. Open the context menu of a user group and select *Account Manager*.
4. Select the checkbox against *Database Credentials* and then select *Add*.
5. Enter the values for the required fields.
6. Select *Save & Close*.

Results

You've successfully defined a new data source reference with the database credentials for the members of the user group. You can go to the *Properties* of any user in this user group to check the data source reference that you have updated now.

10.1.5 Associate data source reference in OLAP connection

Context

An administrator gets an option to select the data source reference of their choice when Credential Mapping is selected as the mode of authentication for a connection.

Follow the steps below to associate a data source reference to a connection.

Procedure

1. Log in to CMC.
2. Go to *OLAP Connections*.
3. Open an existing connection or create a new connection.
4. In the *Authentication* field, choose *Credential Mapping*.
   A field *Data Source Reference* appears.
5. Choose a data source reference.
6. Enter the other required details and select *Save*.

Results

You've successfully associated a data source reference in an OLAP Connection.

10.1.6 Secondary Credentials — Key Rotation Administration

Encryption key rotation for secondary credentials protects stored authentication data by periodically replacing encryption keys while maintaining access to existing credentials. Use this feature to enhance security compliance and respond to potential key compromise without service disruption.

This section describes how encryption key rotation works for secondary credentials, which console commands manage keys, and the procedures for the common operational scenarios.

Managing Key Rotation

The CMS encrypts each secondary credential with an encryption key. It stores the encryption keys in a hidden location in the CMS database, where they don't appear in the *Central Management Console (CMC)*. Only the CMS server process can read or write these keys.

Each encrypted credential value includes the identifier (`SI_ID`) of the key that encrypted it. When the CMS reads a credential, it finds the matching key object. When you rotate in a new key, the CMS keeps the previous keys in a *Deactivated*state, so old credentials remain readable. The CMS retains these deactivated keys until it re-encodes all credentials that reference them with the current active key.

Key states

State	Meaning
Active	The key encrypts all new credentials. Only one key is Active at a time.
Deactivated	This encryption method is no longer used for new credentials. However, the system retains it to decrypt existing credentials.
RekeyInProgress	The system queues the key for re-encoding. The CMS migrates the remaining credentials away from this key.
Destroyed	No credentials reference this key. The system retains the most recent *Destroyed* keys as a safety measure. The system removes only the oldest keys beyond this limit when CMS restarts.

Key types

Type	Description
Auto	The CMS automatically creates this encryption key. The system uses a randomly generated 32-byte AES-256 key. The key expires after 30 days, and the system renews it automatically.
Manual	The key does not expire. This is suitable when multiple CMS applications must share the same key. For example, use this key when promoting users between organizations.

Automatic rotation (auto keys)

The CMS renews auto keys automatically without administrator intervention:

- During startup, if no key exists, the CMS automatically creates the first auto key.
- The CMS periodically checks whether the active auto key has passed its expiration date (30 days by default). When the key expires, the CMS creates a new auto key immediately and changes the old key status to *Deactivated*.
- The CMS re-encodes any credentials that still reference *Deactivated* keys in the background. When a *Deactivated* key has zero credential references, the CMS changes its status to *Destroyed*. The most recent *Destroyed* keys are kept as a safety margin. Older keys are removed on the next CMS restart.

The credentials remain available throughout the rotation process. Credentials encrypted with a *Deactivated* key remain decryptable until re-encoding is complete.

Background re-encoding

The system triggers re-encoding when required. When the number of *Deactivated* auto keys exceeds the internal limit (2), the system promotes the oldest keys to the *RekeyInProgress* status. The CMS then begins re-encoding credentials in the background. The system processes all user objects, re-encrypts any credential not on the current active key, and then moves zero-reference keys to the *Destroyed* status. The operation stops safely when the CMS shuts down.

Console Commands

All key-management operations are available through the CMS console under the *2ndcreds key* command family. Connect to the CMS console and run the following commands.

List keys

```
2ndcreds key list
```

This command displays all encryption keys with the following columns:

Column	Description
`SI_ID`	A unique numeric identifier for the key object. Used in other commands.
`State`	The key can have one of the following states: active, deactivated, rekey-in-progress, or destroyed.
`Type`	auto (randomly generated) or manual (passphrase-derived).
`Created`	The timestamp when the key was created.
`Expires`	The expiry timestamp applies to auto keys. Manual keys do not expire.
`VirtualID`	A cross-system identity handle that appears only for manual keys.
`Verification`	A verification code is required for manual keys and auto keys.

Creating a New Auto Key Immediately

```
2ndcreds key auto
```

This command rotates the key immediately without waiting for it to expire. The existing active key moves to *Deactivated* status. Use this command to rotate the key on demand; for example, as part of a security incident response.

Creating a manual key

```
2ndcreds key manual
```

Enter a passphrase when prompted. The system derives a 32-byte AES-256 key from your passphrase. The console prints a *verification code* that can be shared with another CMS administrator to confirm that both systems use the same passphrase.

To install the same manual key on a second CMS system for cross-system credential sharing, use the extended form:

```
2ndcreds key manual <virtualId> <verificationCode>
```

You obtain the `virtualId` and `verificationCode` from the system's `2ndcreds key list` command output. The command validates the verification code before it creates the key. If the passphrase does not match, the key creation fails immediately and no key object is persisted.

Activating a manual key

```
2ndcreds key activate <id>
```

This command promotes a *Deactivated* manual key to *Active*, making it the only key that the system uses for all new credential encryption. The system moves all previously active keys to *Deactivated* in the same operation. You can activate only manual keys with this command. You cannot activate automatic keys.

Adjusting the expiry time of an auto key

```
2ndcreds key ttl <id> <N>[d|h|m|s]
```

Sets the expiration of an auto key to the current time plus a specified duration (N). You can optionally add a unit suffix to specify the time unit. If you do not include a suffix, the system uses days (d) by default.

Examples:

Command	Effect
`2ndcreds key ttl 7102 30`	Expires in 30 days
`2ndcreds key ttl 7102 30d`	Expires in 30 days
`2ndcreds key ttl 7102 12h`	Expires in 12 hours
`2ndcreds key ttl 7102 1s`	Expires in 1 second (useful for testing)

10.1.6.1 Operational Scenarios

Encryption key management scenarios for CMS secondary credentials, covering new installations, legacy migrations, and transitions between automatic and manual key modes. Use these procedures to bootstrap encryption keys, migrate existing credentials, or synchronize keys across multiple CMS systems.

Scenario 1: New installation or upgrade without credentials

*When this applies:*When you install the CMS for the first time or upgrade from a previous version on a system with no stored secondary credentials.

What happens automatically:

- When you start the CMS for the first time after installation or upgrade, it detects that no encryption key exists.
- The CMS creates the first encryption key and stores it securely in the database.
- The CMS is immediately ready to accept new secondary credentials without requiring any action from you.

Verify the bootstrap:

```
2ndcreds key list
```

Expected output: The system returns exactly one active key of type auto.

SI_ID	State	Type	Created	Expires	Virtual ID	Verification
7102	active	auto	2026-05-21 10:00:00	2026-06-20 10:00:00	-	-

No further action is needed. The key is renewed automatically before it expires.

Scenario 2: Upgrade with existing secondary credentials (legacy migration)

When this applies: The CMS is being upgraded from a version that stored secondary credentials using a legacy key. Users already have secondary credentials stored in the database.

What happens automatically:

- On the first start-up after you upgrade, the CMS detects that credentials exist but were encrypted with the legacy key.
- The CMS does *not* automatically create an encryption key because it cannot determine whether you intend to use automatic or manual key management.
- Legacy credentials remain readable using the legacy key until you create a new encryption key and the migration completes.

Administrator action required: You must create an encryption key before the migration can proceed. Choose one of the following options:

- `2ndcreds key auto` :The system manages key rotation automatically (recommended for most installations).
- `2ndcreds key manual`: You supply a passphrase to derive a key. Use this option when sharing credentials across multiple systems.

Once an active key exists, the CMS re-encodes all legacy credentials in the background, processing one user account at a time. Your credentials remain readable throughout this process, and the CMS continues normal operations.

Monitor the migration:

After you create a key, run the following command:

```
2ndcreds key list
```

While migration is in progress, the active auto key shows a growing number of credential references. To view this information, run the following command:

```
2ndcreds key stats
```

When migration is complete, no credentials reference the legacy key.

SI_ID	State	Credentials
7102	active	42

If the number of legacy-key credentials does not decrease within the expected time frame, check the CMS server log for errors related to the credential migration.

> **Note**
>
> If you downgrade CMS after this upgrade, the older version cannot read the re-encoded credentials because it does not support the managed key infrastructure. Before you complete the migration, verify that downgrade is not required.

Scenario 3: Transition from automatic to manual keys

When this applies: Use this process when you want to control the encryption key manually, for example, to synchronize keys across multiple CMS organizations or to manage key material outside the automatic rotation cycle.

This process involves three steps: creating a manual key, activating it, and optionally re-encoding all existing credentials to eliminate dependency on the previous automatic key.

Step 1 — Create the manual key

```
2ndcreds key manual
```

Enter and confirm a strong passphrase when prompted. The console displays a verification code, for example,

```
Manual key created. SI_ID=7201, VirtualID=7201, Verification=A3F2C1D8
```

Record the *SI_ID*, *VirtualID*, and *Verification* values. You need these values to install the same key on other CMS systems.

After you complete this step, the manual key is *deactivated*. The existing auto key remains active and continues to encrypt new credentials. The system has not re-encoded any credentials yet.

Confirm with:

```
2ndcreds key list
```

SI_ID	State	Type	Created	Expires	Virtual ID	Verification
7102	active	auto	2026-05-21 10:00:00	2026-06-20 10:00:00	-	-
7201	deactivated	manual	2026-05-21 11:00:00	-	7201	A3F2C1D8

Step 2 — Activate the manual key

```
2ndcreds key activate 7201
```

This action promotes the manual key to *Active* and the auto key is *deactivated*. The system uses the manual key for all new credential encryption.

Confirm with:

```
2ndcreds key list
```

SI_ID	State	Type	Created	Expires	Virtual ID	Verification
7102	deactivated	auto	2026-05-21 10:00:00	2026-06-20 10:00:00	-	-
7201	active	manual	2026-05-21 11:00:00	-	7201	A3F2C1D8

Your existing credentials encrypted with the automatic key (SI_ID 7102) remain readable. The system reencodes them in the background.

Step 3 (optional) — Force immediate re-encoding of all credentials

By default, the system re-encodes credentials only when needed. To force all credentials to use the manual key immediately, run the following command (for example, before decommissioning the auto key):

```
2ndcreds recode
```

After the command completes, verify that no credentials reference the old auto key:

```
2ndcreds key stats
```

SI_ID	State	Credentials
7102	deactivated	0
7201	active	42

When a deactivated auto key has zero references, the CMS moves it to *Destroyed*. The CMS retains the most recent destroyed keys as a safety margin. The CMS removes older keys beyond this limit on the next restart.

Installing the same manual key on a second CMS system

On the second CMS system, run the following command:

```
2ndcreds key manual 7201 A3F2C1D8
```

Enter the *same passphrase* used on the first system. The command validates the verification code before creating any key object. If the code does not match, the command fails without making changes.

Next, activate the manual key on the second system by running the following command:

```
2ndcreds key activate <id>
```

Both systems now share the same derived key material. When you promote users from one system to the other, the destination system automatically decrypts their secondary credentials.

Reverting to automatic mode

To return to automatic key management, run the following command:

```
2ndcreds key auto
```

The system immediately creates a new automatic key and sets it to *Active*. Your manual key moves to *deactivated* status. Automatic expiration and renewal resume from this point.

10.1.6.2 Summary of Commands

Command reference table for managing encryption keys in the `2ndcreds` system. Use these commands to create, activate, rotate, and monitor encryption keys that protect stored credentials.

Command	Purpose
`2ndcreds key list`	Lists all key objects, including their state, type, expiry date, and verification status.
`2ndcreds key auto`	Creates a new automatic key immediately and forces rotation.
`2ndcreds key manual`	Creates a manual key from a passphrase. This generates a new standalone key.
`2ndcreds key manual <vid> <code>`	Creates a manual key and verifies that it matches another system.
`2ndcreds key activate <id>`	Changes a Deactivated manual key to Active status.
`2ndcreds key ttl <id> <N>[d|h|m|s]`	Adjusts the expiry time of an automatic key.
`2ndcreds key stats`	Shows credential reference counts for each key.
`2ndcreds recode`	Re-encodes all credentials onto the current active key immediately.

11 Server Administration

11.1 Working with the Servers management area in the CMC

The Servers management area of the CMC is your primary tool for server management tasks. It provides a list of all of the servers in your deployment. For most management and configuration tasks, you need to select a server in the list and choose a command from the Manage or Action menu.

About the navigation tree

The navigation tree on the left side of the Servers management area provides a number of ways to view the Servers list. Select items in the navigation tree to change the information displayed in the *Details* pane.

Navigation tree option	Description
Servers List	Displays a complete list of all servers in the deployment.
Server Groups List	Displays a flat list of all available server groups in the Details pane. Select this option if you want to configure a server group's settings or security.
Server Groups	Lists the server groups and the servers within each server group. When you select a server group, its servers and server groups are displayed in the Details pane in a hierarchical view.
Nodes	Displays a list of the nodes in your deployment. Nodes are configured in the CCM. You can select a node by clicking it to view or manage the servers on the node.

Navigation tree option	Description
Service Categories	Provides a list of the types of services that may be in your deployment. Service categories are divided into core BI platform services and services associated with specific SAP BusinessObjects components. Service categories include: • *Connectivity Services* • *Core Services* • *Crystal Reports Services* • *Data Federation Services* • *Promotion Management Services* • *Analysis Services* • *Web Intelligence Services* Select a service category in the navigation list to view or manage the servers in the category. **Note** A server may host services belonging to multiple service categories. Therefore a server can appear in several service categories.
Server Status	Displays the servers according to their current status. This is a valuable tool for checking to see which of your servers are running or stopped. If you are experiencing slow performance on the system, for example, you can use the *Server Status* list to quickly determine if any of your servers are in an abnormal state. Possible server states include the following: • *Stopped* • *Starting* • *Initializing* • *Running* • *Stopping* • *Running with Errors* • *Failed* • *Waiting for resources*

About the Details pane

Depending on which options you have selected in the navigation tree, the *Details* pane on the right side of the Servers management area shows a list of servers, server groups, states, categories, or nodes. The following table describes the information listed for servers in the *Details* pane.

Note

For nodes, server groups, categories, and states, the *Details* pane usually shows names and descriptions.

Details pane column	Description
Server Name or *Name*	Displays the name of the server.
State	Displays the current status of the server. You can sort by server state using the *Server Status* list in the navigation tree. Possible server states include the following: • *Stopped* • *Starting* • *Initializing* • *Running* • *Stopping* • *Running with Errors* • *Failed* • *Waiting for resources*
Enabled	Displays whether the server is enabled or disabled.
Stale	If the server is marked as *Stale*, then it requires a restart. For example, if you change certain server settings in the server's *Properties* screen, you may need to restart the server before the changes will take effect.
Kind	Displays the type of server.
Host Name	Displays the Host Name for the server.
Health	Indicates the general health of the server. Possible server states include the following: • *Green* (healthy) • *Amber* (caution) • *Red* (danger) The health state of a server directly depends on the status of the server's watch. For example, the health state of the Central Management Server depends on the status of the `<NODENAME>.CentralManagementServer Watch`. You can access the details of watches on the *Monitoring* page in the CMC: on the *Watchlist* tab, select the watch and click *Edit*. You will see the *Caution Rule* and *Danger Rule* for the watch, which map to the amber and red health states, respectively.
PID	Displays the unique Process ID number for the server.
Description	Displays a description of the server. You can change this description in the server's *Properties* page.
Date Modified	Displays the date that the server was last modified, or when the server's state was changed. This column is very useful if you want to check the status of recently changed servers.

11.2 Managing servers by using scripts on Windows

The `ccm.exe` executable lets you start, stop, restart, enable, and disable the servers in your Windows deployment through the command line.

Related Information

ccm.exe [page 1011]

11.3 Managing servers on Unix

The `ccm.sh` executable lets you start, stop, restart, enable, and disable the servers in your Unix deployment through the command line.

Related Information

ccm.sh [page 1004]

11.4 Viewing and changing a server's status

11.4.1 Viewing the state of servers

The status of a server is its current state of operation: a server can be running, starting, stopping, stopped, failed, initializing, started with errors, or waiting for resources. To respond to BI platform requests, a server must be running and enabled. A server that is disabled is still running as a process; however, it is not accepting requests from the rest of the BI platform. A server that is stopped is no longer running as a process.

This section shows how to modify the state of servers by using the CMC.

Related Information

To view a server's status [page 406]
To view the state of services [page 406]
Starting, stopping, and restarting servers [page 407]

Enabling and disabling servers [page 410]
Stopping a Central Management Server [page 409]
To automatically start a server [page 409]

11.4.1.1 To view a server's status

Procedure

1. Go to the *Servers* management area of the CMC.

   The *Details* pane displays the service categories in your deployment.
2. To view a list of servers in a given Server Group, Node, or Service Category, in the navigation tree click the server group, node, or category.
   The *Details* pane displays the list of servers in your deployment. The *State* column provides the status for each server in the list.
3. If you want to view a list of all of the servers that currently have a particular status, expand the *Server Status* option in the navigation tree and select the status you want.

   A list of servers with the selected status appears in the Details pane.

   > ⓘ Note
   >
   > This can be particularly useful if you need to quickly view a list of servers that are not starting properly or have stopped unexpectedly.

11.4.1.2 To view the state of services

Prerequisites

If any service fails, the state of the host server is set to either *Running with Errors* (meaning that at least one service started successfully) or *Failed* (meaning that none of the services started successfully). You can view the server states in the CMC and CCM. However, you can also view the status of individual services, on the server's *Properties* page in the CMC.

Procedure

1. Go to the *Servers* management area of the CMC.

   The *Details* pane displays the service categories in your deployment.
2. To view a list of servers in a given Server Group, Node, or Service Category, in the navigation tree click the server group, node, or category.
   The *Details* pane displays the list of servers in your deployment.

3. Double-click a server to open its *Properties* page.

   The *Properties* page shows the properties for the server and the services it hosts. For failed services, error messages are also displayed.

Related Information

Viewing the state of servers [page 405]

11.4.2 Starting, stopping, and restarting servers

Starting, stopping, and restarting servers are common actions that you perform when you configure servers or take them offline. For example, if you want to change the name of a server, then you must first stop the server. Once you have made your changes, you start the server again to effect your changes. If you make changes to a server's configuration settings, the CMC will prompt you if you need to restart the server.

The remainder of this section tells you when a certain configuration change requires that you first stop or restart the server. However, because these tasks appear frequently, the concepts and differences are explained first, and the general procedures are provided for reference.

Action	Description
Stopping a server	You may need to stop BI platform servers before you can modify certain properties and settings.
Starting a server	If you stopped a server to configure it, you must restart the server before your changes will take effect and before the server can resume processing requests.
Restarting a server	Restarting a server is a shortcut to stopping a server completely and then starting it again. If you need to restart a server after changing a server setting, you will be prompted by the CMC.
Starting a server automatically	You can set servers to start automatically when the Server Intelligence Agent starts.
Force Termination	Stops a server immediately (whereas when you stop a server, it will stop when it has completed its current processing activities). Forcibly terminate a server only when stopping the server has failed and you need to stop the server immediately.

> → Tip
>
> When you stop (or restart) a server, you terminate the server's process, thereby stopping the server completely. Before you stop a server, it is recommended that you

- Disable the server so it can finish processing any jobs it has in progress, and
- Ensure that there are no auditing events remaining in the queue. To view the number of auditing events remaining in the queue, navigate to the server's *Metrics* screen and view the *Current Number of Auditing Events in the Queue* metric.

Related Information

Enabling and disabling servers [page 410]

11.4.2.1 To start, stop, or restart servers with the CMC

Procedure

1. Go to the *Servers* management area of the CMC.

   The *Details* pane displays the service categories in your deployment.
2. To view a list of servers in a particular Server Group, Node, or Service Category, select the group, node, or category on the navigation pane.
   The *Details* pane displays a list of servers.
3. If you want to view a list of all of the servers that currently have a particular status, expand the *Server Status* option in the navigation tree and select the status you want.

   A list of servers with the selected status appears in the *Details* pane.

   > ⓘ Note
   >
   > This can be particularly useful if you need to quickly view a list of servers that are not starting properly or have stopped unexpectedly.
4. Right-click the server whose status you want to change, and depending on the action you need to perform select *Start Server*, *Restart Server*, *Stop Server*, or *Force Termination*.

11.4.2.2 To start, stop, or restart a Windows server with the CCM

Procedure

1. In the CCM, click the *Manage Servers* button on the toolbar.
2. When prompted, log on to your CMS with an administrative account.
3. In the *Manage Servers* dialog box, select the server that you want to start, stop, or restart.

4. Click *Start*, *Stop*, *Restart*, or *Force Terminate*.
5. Click *Close* to return to the CCM.

11.4.2.3 To automatically start a server

Context

By default, servers in your deployment are automatically started when the Server Intelligence Agent starts. This task shows where to set the autostart option.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the server you want to automatically start.
   The *Properties* screen appears.
3. Under *Common Settings*, select the *Automatically start this server when the Server Intelligence Agent starts* check box, and click *Save* or *Save & Close*.

> **Note**
>
> If the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster, you must use the CCM to restart the system. After using the CCM to stop the SIA, right-click the SIA and select *Properties*. On the *Startup* tab, click *Properties* to open the Server Properties page for the CMS. Select *Auto-Start*, then click *OK* to close the Server Properties page, and then click *OK* again. Restart the SIA. The *Autostart* option is available only when the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster.

11.4.3 Stopping a Central Management Server

If your BI platform installation has more than one active Central Management Server (CMS), you can shut down a single CMS without losing data or affecting system functionality. Another CMS on the node will assume the workload of the stopped server. Clustering multiple CMSs enables you to perform maintenance on each of your Central Management Servers in turn without taking the BI platform out of service.

However, if your BI platform deployment has a single CMS, shutting it down will make the BI platform unavailable to your users and will interrupt the processing of reports and programs. To avoid this problem, the Server Intelligence Agent for each node ensures that at least one CMS is running at all times. You can still stop a CMS by stopping its SIA, but before stopping the SIA, you should disable the processing servers via the CMC so that they can finish any jobs in progress before the BI platform shuts down, because all other servers on the node will also shut down.

> **Note**
>
> You may encounter situations where the CMS has been stopped and you need to restart the system from the CCM. For example, if you shut down each CMS on a node and the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster when the SIA starts, you must use the CCM to restart the system. In the CCM, right-click the SIA and choose *Properties*. On the *Startup* tab, click *Properties* to open the Server Properties page for the CMS. Select *Auto-Start*, then click *OK* to close the Server Properties page, and then click *OK* again. Restart the SIA. The *Autostart* option is available only when the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster.

If you want to configure your system so that you can start and stop the Central Management Server in the cluster without starting and stopping other servers, put the CMS on a separate node. Create a new node and clone the CMS to the node. With the CMS on its own node, you can easily shut down the node without affecting other servers.

Related Information

Using nodes [page 455]
Cloning servers [page 412]
Clustering Central Management Servers [page 416]

11.4.4 Enabling and disabling servers

When you disable a BI platform server, you prevent it from receiving and responding to new BI platform requests, but you do not actually stop the server process. This is useful when you want to allow a server to finish processing all of its current requests before you stop it completely.

For example, you may want to stop a Job Server before rebooting the machine it is running on. However, you want to allow the server to fulfill any outstanding report requests that are in its queue. First, you disable the Job Server so it cannot accept any additional requests. Next, go to the Central Management Console to monitor when the server completes the jobs it has in progress. (From the *Servers* management area, right-click the server and select *Metrics*.) Then, once it has finished processing current requests, you can safely stop the server.

> **Note**
>
> The CMS must be running in order for you to enable and/or disable other servers.

> **Note**
>
> A CMS cannot be enabled or disabled.

11.4.4.1 To enable and disable servers with the CMC

Procedure

1. Go to the *Servers* management area of the CMC.
2. Right-click the server whose status you want to change, and depending on the action you need to perform click *Enable Server* or *Disable Server*.

11.4.4.2 To enable or disable a Windows server with the CCM

Procedure

1. In the CCM, click *Manage Servers*.
2. When prompted, log on to your CMS with the credentials that provide you with administrative privileges to the BI platform.
3. In the *Manage Servers* dialog box, select the server that you want to enable or disable.
4. Click *Enable* or *Disable*.
5. Click *Close* to return to the CCM.

11.5 Adding, cloning, or deleting servers

11.5.1 Adding, cloning, and deleting servers

If you want to add new hardware to the BI platform by installing server components on new, additional machines, run the BI platform installation program on those machines. The setup program allows you to perform a Custom installation. During the Custom installation, specify the CMS from your existing deployment, and select the components that you want to install on the local machine. For details on custom installation options, see the *SAP BI platform Installation Guide*.

11.5.1.1 Adding a server

Prerequisites

You can run multiple instances of the same BI platform server on the same machine. To add a server:

Procedure

1. Go to the *Servers* management area of the CMC.
2. On the *Manage* menu, click *New* > *New Server*.
   The *Create New Server* dialog box appears.
3. Choose the *Service Category*.
4. Choose the type of service that you need from the *Select Service* list, then click *Next*.
5. To add an additional service to the server, select the service in the *Available Additional Services* list and click >.

   > **Note**
   >
   > Additional services are not available for all server types.

6. After adding the additional services you want, click *Next*.
7. If your BI platform architecture is composed of multiple nodes, choose the node where you want to add the new server from the *Node* list.
8. Type a name for the server in the *Server Name* box.

   Each server on the system must have a unique name. The default naming convention is `<NODENAME>.<servertype>` (a number is appended if there is more than one server of the same type on the same host machine).
9. To include a description for the server, type it into the *Description* box.
10. If you are adding a new Central Management Server, specify a port number in the *Name Server Port* field.
11. Click *Create*.
    The new server appears in the list of servers in the *Servers* area of the CMC, but it is neither started nor enabled.
12. Use the CMC to start and enable the new server when you want it to begin responding to BI platform requests.

11.5.1.2 Cloning servers

If you want to add a new server instance to your deployment, you can clone an existing server. The cloned server retains the configuration settings of the original server, except the Common Settings and Command Line Parameters. This can be particularly useful if you are expanding your deployment and want to create new server instances that use almost all of the same server configuration settings as an existing server.

Cloning also simplifies the process of moving servers between nodes. If you want to move an existing CMS to another node, you can clone it to the new node. The cloned CMS appears on the new node and retains all of the configuration settings of the original CMS, except Common Settings and Command Line Parameters.

There are some considerations to keep in mind when cloning servers. You may not want all settings to be cloned, so it's good practice to check the cloned server to make sure it meets your needs.

> **Note**
>
> Before you clone servers, make sure that all machines in your deployment have the same version of BI platform (and any updates, if applicable).

> **Note**
>
> You can clone servers from any machine. However, you can only clone servers to machines where the required binaries for the server are installed.

> **Note**
>
> When you clone a server, it does not necessarily mean that the new server will use the same OS credentials. The user account is controlled by the Server Intelligence Agent that the server is running under.

11.5.1.2.1 Using placeholders for server settings

Placeholders are node-level variables that are used by the servers that are running on the node. Placeholders are listed on a dedicated page in the Central Management Console (CMC). When you double-click any server listed under *Servers* in the CMC, a link is provided on the left-hand navigation pane for "Placeholders". The *Placeholders* page lists all the available placeholder names and their associated values for the selected server. Placeholders contain read-only values and the placeholder names begin and end with the percentage character %.

> **Note**
>
> You can always overwrite a placeholder setting with a specific string in the CMC Server *Properties* page.

Example

Placeholders are useful when cloning servers. For example, multi-drive machine A has the BI platform installed on `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. So the `%DefaultAuditingDir%` placeholder will be `D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

On another machine, machine B, there is only one disc drive (no drive D) and the BI platform is installed on `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. In this case the `%DefaultAuditingDir%` placeholder will be `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

To clone the Event Server from machine A to machine B, if placeholders are used for the Auditing Temporary Directory, the placeholders will resolve themselves and the Event Server will work properly. If no placeholders are used, the Event Server will fail unless you manually overwrite the Auditing Temporary Directory setting.

11.5.1.2.2 To clone a server

Procedure

1. On the machine that you want to add the cloned server to, go to the *Servers* management area of the CMC.
2. Right-click the server that you want to clone and select *Clone Server*.
   The *Clone Server* dialog box appears.
3. Type a name for the server (or use the default name) in the *New Server Name* field.
4. If you are cloning a Central Management Server, specify a port number in the *Name Server Port* field.
5. On the *Clone to Node* list, choose the node where you want to add the cloned server, then click *OK*.
   The new server appears in the *Servers* management area of the CMC.

11.5.1.3 Deleting a server

Context

Procedure

1. Go to the *Servers* management area of the CMC.
2. Stop the server that you want to delete.
3. Right-click the server and select *Delete*.
4. When prompted for confirmation, click *OK*.

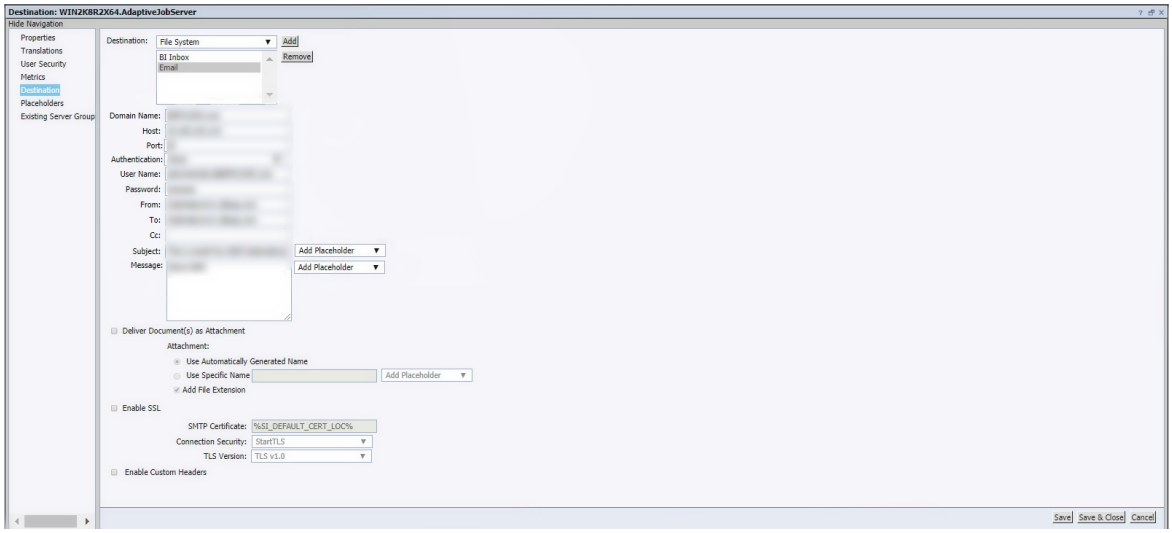
11.6 Add Custom Internet Headers

Context

Internet header of an email message comprises information about the composer of the message, the email server the message has passed through, and the tool or software used to compose the message. You can now add custom internet headers to the emails scheduled from SAP BusinessObjects BI platform. Follow the steps below to add custom headers:

Procedure

1. Log in to *CMC*.
2. Go to *Servers* and then *Servers List*.
3. Open the context menu for *Adaptive Job Server* and choose *Destinations*.
4. In the *Destination* wizard, choose *Email* and add the required details for each field as shown below:



5. Check *Enable Custom Headers* and add the internet headers in the blank field as shown below:

6. Choose *Save and Close*.

Results

The emails with scheduled documents now contain the internet headers.

> **Note**
>
> - While scheduling, choose *Use Default Settings* to add custom internet headers in the scheduled emails.
> - Every *Adaptive Job Server* should be configured to ensure that custom headers are added in every email.

11.7 Clustering Central Management Servers

11.7.1 Clustering Central Management Servers

If you have a large or mission-critical implementation of SAP BusinessObjects Business Intelligence platform, you will probably want to run several CMS machines together in a cluster. A cluster consists of two or more CMS servers working together against a common CMS system database. If a machine that is running one CMS fails, a machine with another CMS will continue to service BI platform requests. This "high availability" support helps to ensure that BI platform users can still access information when there is an equipment failure.

This section shows how to add a new CMS cluster member to a production system that is already up and running. When you add a new CMS to an existing cluster, you instruct the new CMS to connect to the existing CMS system database and to share the processing workload with any existing CMS machines. For information about your current CMS, go to the *Servers* management area of the CMC.

Before clustering CMS machines, you must make sure that each CMS is installed on a system that meets the detailed requirements (including version levels and patch levels) for operating system, database server, database access method, database driver, and database client outlined in the Product Availability Matrix.

In addition, you must meet the following clustering requirements:

- For best performance, the database server that you choose to host the system database must be able to process small queries very quickly. The CMS communicates frequently with the system database and sends it many small queries. If the database server is unable to process these requests in a timely manner, BI platform performance will be greatly affected.
- For best performance, run each CMS cluster member on a machine that has the same amount of memory and the same type of CPU.
- Configure each machine similarly:
  - Install the same operating system, including the same version of operating system service packs and patches.
  - Install the same version of the BI platform (including patches, if applicable).
  - Ensure that each CMS connects to the CMS system database in the same manner: whether you use native or ODBC drivers. Make sure that the drivers are the same on each machine, and are a supported version.
  - Ensure that each CMS uses the same database client to connect to its system database and that it is a supported version.
  - Check that each CMS uses the same database user account and password to connect to the CMS system database. This account must have create, delete, and update rights on the system database.
  - Ensure that the nodes on which each CMS is located are running under the same operating system account. (On Windows, the default is the "LocalSystem" account.)
  - Verify that the current date and time are set correctly on each CMS machine (including settings for daylight savings time).
  - Ensure that all machines in a cluster (including the machines that host the CMS) are set to the same system time. For best results, synchronize the machines to a time server (such as `time.nist.gov`) or use a central monitoring solution.
  - Ensure that the same WAR files are installed on all web application servers in the cluster. For more information on WAR file deployment, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*.

- Ensure that each CMS in a cluster is on the same Local Area Network.
- Out-of-Band threads (-oobthreads) are used by clustering pings and clustering notifications. Since both operations are quick (notifications are asynchronous), the BI platform no longer requires multiple oobthreads and only one -oobthread is created.
  If your cluster has more than eight CMS cluster members, ensure that the command line for each CMS includes the `-oobthreads <numCMS>` option, where `<numCMS>` is the number of CMS servers in the cluster. This option ensures that the cluster can handle heavy loads. For information about configuring server command lines, see the server command lines appendix in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
- Enabling auditing to a single CMS itself will act as a configuration in a clustered environment. You can also change the auditing database details in the Audit settings page in CMC. The requirements for the auditing database are the same as those for the system database in terms of database servers, clients, access methods, drivers, and user IDs.

> → Tip
>
> By default, a cluster name reflects the machine host-name of the first CMS that you install.

Related Information

Changing the name of a CMS cluster [page 419]

11.7.1.1 Adding a CMS to a cluster

There are several ways to add a new CMS cluster member. Follow the appropriate procedure:

- You can install a new node with a CMS on a new machine.
- If you already have a node with CMS binary files, then you can add a new CMS server from the CMC.
- If you already have a node with CMS binary files, you can also add a new CMS server by cloning an existing CMS server.

> ⓘ Note
>
> Back up your current CMS system database, server configuration, and the contents of your Input and Output File Repositories before making any changes. If necessary, contact your database administrator.

Related Information

Adding a new node to a cluster [page 418]
Adding a server [page 411]
Cloning servers [page 412]
Overview of backup and restore [page 499]

11.7.1.2 Adding a new node to a cluster

When you add a node (a node is a collection of BI platform servers managed by a single Server Intelligence Agent), you are prompted to either create a new CMS or to cluster the node to an existing CMS.

If you want to cluster a node to an existing CMS, you can also use the installation setup program. Run the BI platform installation and setup program on the machine where you want to install the new CMS cluster member. The setup program allows you to perform a custom installation. During the custom installation, specify the existing CMS whose system you want to expand, and select the components that you want to install on the local machine. In this case, specify the name of the CMS that is running on your existing system, choose to install a new CMS on the local machine, and provide the setup program with the information it needs to connect to your existing CMS system database. When the setup program installs the new CMS on the local machine, it automatically adds the server to your existing cluster.

> **Note**
>
> Before you cluster a new node to an existing CMS, if the new node is a brand new server, ensure that the BI platform installation on that server is at the same patch level as the existing BI platform environment.

> **Note**
>
> Edge BI and Crystal Server licenses don't allow clustering or multi-node deployment. However, as of Edge BI 4.3 SP2 and Crystal Server 2020 SP2, if Edge BI and Crystal Server are deployed on Linux, ONE Windows node with Crystal Reports 2020 services is allowed. See How to distribute SAP Crystal Reports 2025 services to a Windows server for more information.

Related Information

Using nodes [page 455]

11.7.1.3 Adding clusters to the web application property files

If you have added additional CMSs to your deployment, then that information is captured in `clusterinfo.1400.properties` file available at `C:/Users/<you_user>/.businessobjects`. This file is generated or updated when you restart the SIA.

> **Note**
>
> In a stand-alone Tomcat deployment, the `clusterinfo.1400.properties` file gets generated only when you log in with one of the CMS name. When you update the cluster, the file in a stand-alone Tomcat deployment is not updated. You need to copy the file from your CMS to your Tomcat machine.

11.7.1.4 Changing the name of a CMS cluster

This procedure allows you to change the name of a cluster that is already installed. After changing the name of the CMS cluster, the Server Intelligences Agent automatically reconfigures each SAP Business Objects server so that it registers with the CMS cluster, rather than with an individual CMS.

> **Note**
>
> For experienced administrators of the BI platform, note that you can no longer use the `-ns` option on the server command line to configure which CMS a server should register with. This is now handled automatically by the SIA.

11.7.1.4.1 To change the cluster name on Windows

Procedure

1. Use the CCM to stop the Server Intelligence Agent for the node that contains a Central Management Server that is a member of the cluster whose name you want to change.
2. Right-click the Server Intelligence Agent and choose *Properties*.
3. In the Properties dialog box, click the *Configuration* tab.
4. Select the *Change Cluster Name to* check box.
5. Type the new name for the cluster.
6. Click *OK* and then restart the Server Intelligence Agent.

   The CMS cluster name is now changed. All other CMS cluster members are dynamically notified of the new cluster name (although it may take several minutes for your changes to propagate across cluster members).
7. Go to the *Servers* management area of the CMC and check that all of your servers remain enabled. If necessary, enable any servers that have been disabled by your changes.

11.7.1.4.2 To change the cluster name on UNIX

Context

Use the `cmsdbsetup.sh` script. For reference, see the “Unix scripts” topic in the Command Line Administration chapter in the *BI platform Administrator Guide*.

Related Information

Unix Scripts [page 1004]

11.8 Managing server groups

Server groups can organize and help to manage BI platform servers on your system. You can select a particular server or server group per publication (not per user), and you can group servers by region or type.

Group servers by region to easily set up default processing settings, recurrent schedules, and scheduling destinations for users who work in a particular regional office. You can associate a report object (such as a Crystal report or a Web Intelligence document) with a single server group so the object is always processed by the same servers, and you can associate scheduled report objects with a particular server group to ensure that scheduled objects are sent to the correct printers, file servers, and so on. Server groups are especially useful when maintaining systems that span multiple locations and time zones.

Server groups are especially useful when maintaining systems that span multiple locations and time zones. For example, use server groups to customize your BI platform system for reports viewed in different locations and for different report types. When organizing servers by region, you can perform the following actions for server groups:

- Configure default processing settings
- Configure recurrent schedules
- Configure scheduling destinations for users who work in a particular regional office
- Associate a report object (such as a Crystal report or a Web Intelligence document) with a single server group so the object is always processed by the same servers
- Associate scheduled report objects with a particular server group to ensure that scheduled objects are sent to the correct printers, file servers, and so on

Group servers by type when configuring objects to be processed by servers that are optimized for those objects.

After creating server groups, configure objects to use specific server groups for scheduling or viewing and modifying reports. Use the navigation tree in the *Servers* management area of the CMC to view server groups. The *Server Groups List* option displays a list of server groups in the *Details* pane, and the *Server Groups* option allows you to view the servers in the group.

Example: Grouping processing servers by type

For example, processing servers need to communicate frequently with the database containing data for published reports. Placing processing servers close to the database server that they need to access improves system performance and minimizes network traffic. Therefore, for a number of reports that run against a DB2 database, you can create a group of processing servers that process reports only against the DB2 database server. To improve system performance when viewing reports, you can configure the reports to always use this processing server group for viewing.

11.8.1 Creating a server group

To create a server group, you need to specify the name and description of the group, and then add servers to the group.

11.8.1.1 To create a non-exclusive server group

Context

Non-exclusive server groups can contain servers or server groups that are part of any other non-exclusive server group or the common server pool.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Choose *Manage* > *New* > *Create Server Group*.

   The *Create Server Group* dialog box appears.
3. In the *Name* field, type a name for the new group of servers.
4. If you want to include additional information about the server group, type it in the *Description* field.
5. Click *OK*.
6. In the *Servers* management area, click *Server Groups* in the navigation tree and select the new server group.
7. Choose *Add Members* from the *Actions* menu.
8. Select the servers that you want to add to this group; then click > .

   > → Tip
   >
   > Use CTRL + click to select multiple servers.

   > ⓘ Note
   >
   > Servers listed only include servers that are not part of any other exclusive server group.
9. Click *OK*.

   You are returned to the *Servers* management area, which now lists all the servers that you added to the group. You can now change the status, view server metrics, and change the properties of the servers in the group.

11.8.1.2 To create an exclusive server group

Exclusive server groups contain servers or server groups that are not part of any other server group or common server pool. When a Server Group is created as Exclusive Server Group, then the servers part of this group cannot be assigned to any other Server Group (Exclusive or Non Exclusive) and Servers added to Exclusive Server Group are excluded from the common pool. This enables you to create server groups that are isolated from the general load of the BI system.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Choose *Manage* > *New* > *Create Server Group*.

   The *Create Server Group* dialog box appears.
3. In the *Name* field, type a name for the new group of servers.
4. If you want to include additional information about the server group, type it in the *Description* field.
5. Select the *Exclusive Server Group* checkbox.

   > ### Note
   >
   > You can create an exclusive server group only at root level. For a child node, you can create an exclusive server group only if the root or parent server group is exclusive.
   >
   > > ### Example
   > >
   > > Consider this scenario to understand exclusive server groups better:
   > >
   > > Two Job Servers: JS1 and JS2 are part of the common server pool.
   > >
   > > You create an exclusive server group: SG1.
   > >
   > > You add JS1 to SG1.
   > >
   > > You schedule Document (D) by selecting the *Only use servers in the selected group* option.
   > >
   > > Assume that both JS1 and JS2 already have some jobs running.
   > >
   > > **Result:** JS1 is already loaded with some jobs that need to be processed. However, as JS1 is now part of SG1, JS1 only gets requests to process worflows assigned to SG1. That is, JS1 is freed from the general system load.
6. Click *OK*.
7. In the *Servers* management area, click *Server Groups* in the navigation tree and select the new server group.
8. Choose *Add Members* from the *Actions* menu.
9. Select the servers that you want to add to this group; then click > .

   > ### → Tip
   >
   > Use `CTRL` + `click` to select multiple servers.

   > ### Note
   >
   > Servers listed only include servers that are not already part of other server groups or the common server pool.
10. Click *OK*.

    You are returned to the *Servers* management area, which now lists all the servers that you added to the group. You can now change the status, view server metrics, and change the properties of the servers in the group.

11.8.2 Converting an exclusive server group to non-exclusive and vice-versa

11.8.2.1 Converting an exclusive server group to a non-exclusive server group

You can now modify an existing exclusive server group to make it non-exclusive.

Context

To convert a root-level exclusive server group to non-exclusive, perform the following:

Procedure

1. Right-click on the exclusive server group that you want to convert, and select *Properties* from the dropdown.

   Properties dialog box opens. You notice that the *Exclusive Server Group* checkbox is selected.
2. Unselect the *Exclusive Server Group* checkbox.

   A warning message appears.
3. Choose *OK* to confirm the conversion.
4. Choose *Save & Close*.

   You have now converted an exclusive server group to non-exclusive.

   > **Note**
   >
   > You can only convert root-level exclusive server groups to non-exclusive.

11.8.2.2 Converting a non-exclusive server group to an exclusive server group

You can now modify an existing non-exclusive server group to make it exclusive.

Context

To convert a non-exclusive server group that contains **independent** servers and server groups, perform the following:

Procedure

1. Right-click on the non-exclusive server group that you want to convert, and select *Properties* from the dropdown.

   Properties dialog box opens. You notice that the *Exclusive Server Group* checkbox is unselected
2. Select the *Exclusive Server Group* checkbox.

   A success message appears.
3. Choose *OK*.
4. Choose *Save & Close*.

   You have now converted a non-exclusive server group to exclusive.

> ⓘ Note
>
> You can only convert a non-exclusive server group that has independent servers and server groups to exclusive. Independent servers and server groups are those servers and server groups that are not part of any other server group.

11.8.3 Working with server subgroups

Subgroups of servers provide you with a way of further organizing your servers. A subgroup is just a server group that is a member of another server group.

For example, if you group servers by region and by country, then each regional group becomes a subgroup of a country group. To organize servers in this way, first create a group for each region, and add the appropriate servers to each regional group. Then, create a group for each country, and add each regional group to the corresponding country group.

There are two ways to set up subgroups: you can modify the subgroups of a server group, or you can make one server group a member of another. The results are the same, so use whichever method proves most convenient.

11.8.3.1 To add subgroups to a server group

Procedure

1. Go to the *Servers* management area of the CMC.
2. Click *Server Groups* in the navigation tree and select the server group you want to add subgroups to.

   This group is the parent group.
3. Choose *Add Members* from the *Actions* menu.
4. Click *Server Groups* in the navigation tree, select the server groups that you want to add to this group, and then click >.

   > → Tip
   >
   > Use `CTRL` + `click` to select multiple server groups.
5. Click *OK*.

   You are returned to the *Servers* management area, which now lists the server groups that you added to the parent group.

11.8.3.2 To make one server group a member of another

Procedure

1. Go to the *Servers* management area of the CMC.
2. Click the group that you want to add to another group.

   > ⓘ Note
   >
   > For root-level exclusive server groups, all exclusive Server Groups are listed under *Available Server Groups*. You can only select one exclusive server group and move it to *Member of Server Groups*, as an exclusive server group can have only one parent server group.
   >
   > Child-level exclusive server groups do not list any server groups under *Available Server Groups*, as a child exclusive server group can have only one parent.
3. Choose *Add to Server Group* from the *Actions* menu.
4. In the *Available Server Groups* list, select the other groups that you want to add the group to, then click >.

   > → Tip
   >
   > Use `CTRL` + `click` to select multiple server groups.
5. Click *OK*.

11.8.4 Modifying the group membership of a server

You can modify a server's group membership to quickly add the server to (or remove it from) any group or subgroup that you have already created on the system.

For example, suppose that you created server groups for a number of regions. You might want to use a single Central Management Server (CMS) for multiple regions. Instead of having to add the CMS individually to each regional server group, you can click the server's *Member of* link to add it to all three regions at once.

11.8.4.1 To modify a server's group membership

Procedure

1. Go to the *Servers* management area of the CMC.
2. Right-click the server whose membership information you want to change, and select *Existing Server Groups*.
   In the details panel, the *Available Server Groups* list displays the groups you can add the server to. The *Member of Server Groups* list displays any server groups that the server currently belongs to.

   > **Note**
   >
   > For root-level server groups, all Exclusive Server Groups are listed under *Available Server Groups*. You can only select one exclusive server group and move it to *Member of Server Groups*, as an exclusive server group can have only one parent server group. After you select an exclusive server group from *Available Server Groups* and move it to *Member of Server Groups*, the exclusive server group is moved out of its root server group and into a new server group to where it's mapped.
   >
   > For child-level server groups, existing parent server groups are displayed under *Member of Server Groups* and other exclusive server groups are listed under *Available Server Groups*. You can change the mapping of child server group from one exclusive parent to another.
3. To change the groups that the server is a member of, use the arrows to move server groups between the lists, then click *OK*.

Results

> **Note**
>
> *Remove from server group* option is only listed for child-level exclusive server groups. Once a child-level exclusive server group is removed from the parent server group, it will retain its exclusivity and be moved to the root level.
>
> Server groups appear in BI Launch Pad if user security rights are granted by the administrator from the CMC for specific server groups.

11.8.5 Administrative access to servers and server groups for users

Granting administrative rights to users enables them to perform server and server group tasks, such as starting and stopping servers.

Depending on your system configuration and security concerns, you may limit server management to the BI platform administrator or you may need to provide administrative access to other people using those servers. Many organizations have a group of IT professionals dedicated to server management. If your server team needs to perform regular server maintenance tasks that require them to shut down and start up servers, you need to grant them administrative rights to the servers. You may also want to delegate BI platform server administration tasks to other people or want some groups in your organization to control their own server management.

> ⓘ Note
>
> You can select a server or server group for a publication (not for a particular user). However, you can assign administrative rights to users or user groups for a particular server or server group.

11.8.5.1 Granting administrative access rights to a server or a server group

You can assign administrative rights to users or user groups for a particular server or server group.

Context

> ⓘ Note
>
> You can select a server or server group for a publication (not for a user).

Procedure

1. Go to the *Servers* management area of the CMC.
2. Right-click the server or server group for which to grant administrative access rights and select *User Security*.
3. Click *Add Principals* to add users or groups for whom to give administrative rights to the server or server group.
4. In the *Add Principals* dialog box, select a user or group for whom to give administrative rights to the server or server group, and click >.

5. Click *Add and Assign Security*.
6. On the *Assign Security* screen, select security settings for the user or group, and click *OK*.

Related Information

How rights work in BI platform [page 115]

11.8.5.2 Object rights for the Report Application Server

To allow users to create or modify reports over the Web through the Report Application Server (RAS), you must have RAS Report Modification licenses available on your system. You must also grant users a minimum set of object rights. When you grant users these rights to a report object, they can select the report as a data source for a new report or modify the report directly:

- View objects (or "View document instances" as appropriate)
- Edit objects
- Refresh the report's data
- Export the report's data

Users must also have permission to add objects to at least one folder before they can save new reports back to the BI platform.

To ensure that users retain the ability to perform additional reporting tasks (such as copying, scheduling, printing, and so on), it's recommended that you first assign the appropriate access level and update your changes. Then, change the access level to Advanced, and add any of the required rights that are not already granted. For instance, if users already have View On Demand rights to a report object, you allow them to modify the report by changing the access level to Advanced and explicitly granting the additional Edit objects right.

When users view reports through the Advanced DHTML viewer and the RAS, the View access level is sufficient to display the report, but View On Demand is required to actually use the advanced search features. The extra Edit objects right is not required.

11.8.6 Mapping a User Group to a Server Group

You can now map a user group to a particular server group using the new *Default Settings* option.

Context

To map a user group to a server group, perform the following steps:

Procedure

1. Log on to the CMC.
2. Choose *Users and Groups*.
3. In the *Users and Groups* page, right-click on the required user group (which you want to map the server group to).
4. Select *Default Settings*.
5. In the *Scheduling Server Group* page, set the default servers to use for scheduling the user group.

   You can select one of the following options:
   - (Default) Choose *Use the first available server* to run the object on the server with the most resources free at the time of scheduling.
   - Choose *Give preference to servers in the selected group* to run the object on servers in a particular server group. Then select the required server group from the dropdown box to set a preference for a particular server group. If no servers in the selected server group are available, the object is run on the next available server from the common server pool.
   - Choose *Only use servers in the selected group* to run the object only on servers in a particular server group and select the required server group from the dropdown box to exclusively use one server group. If no servers in the selected group are available, the object is not processed. Also, if a job server is not present in the assigned server group, the job remains in the pending state.

> ⓘ Note
>
> You can choose to map an exclusive or non-exclusive server group to a user group by selecting one of the two radio buttons: *Give preference to servers in the selected group* or *Only use servers in the selected group*.
>
> Similarly, you can assign server groups for viewing or processing Crystal Reports and Web Intelligence documents by navigating to *Default Settings* and *Crystal Reports Process Settings* and *Web Intelligence Process Settings* respectively.
>
> If a server group is associated as required, it means that **only** servers from that particular server group are used. Servers from the common pool are not used. If a server group is associated as preferred, then if the servers in the server group are busy, servers from the common server pool are used. Common server pool includes all servers that are not part of any exclusive server group. For more information on exclusive server groups, see To create an exclusive server group [page 421].

Assigning server group to user group can be complex, as one user can be part of multiple user groups. And, each user group can be mapped to different server groups. Each server group can be assigned as either required or preferred.

Example

Consider this scenario:

A user (U) is part of two user groups - UG1 and UG2. And each user group is mapped to a different server group - SG1 and SG2. Then, the results for various scenarios would be:

Scenario	Result
You schedule a document (D). Server group 1 (SG1) is set at UG1 and Server Group 2 (SG2) is set at UG2. SG1 is set as Required (R). SG2 is also set as Required (R). No server group is assigned at document (D) level.	Combination of the two server groups (SG1 and SG2) acts as a Required (R) server group. Since both server groups (SG1 and SG2) are set as Required, servers from the common pool are NOT used.
You schedule a document (D). Server group 1 (SG1) is set at UG1 and Server Group 2 (SG2) is set at UG2. SG1 is set as Preferred (P). SG2 is also set as Preferred (P). No server group is assigned at document (D) level.	Combination of the two server groups (SG1 and SG2) acts as a Preferred (P) server group. Since both server groups (SG1 and SG2) are set as Preferred, then if no servers in the selected groups are available, servers from the common pool are used.
You schedule a document (D). Server group 1 (SG1) is set at UG1 and Server Group 2 (SG2) is set at UG2. SG1 is set as Required (R). SG2 is set as Preferred (P). No server group is assigned at document (D) level.	Combination of the two server groups (SG1 and SG2) acts as a Required (R) server group. Since the combination (SG1 and SG2) acts as a Required server group, servers from the common pool are NOT used.

6. Choose *Save & Close*.

You have now successfully mapped a user group to a server group.

Note

- A user can belong to one or more user group and each of these user groups can belong to other user groups. If no server group is associated with the immediate user group that a user belongs to, then the program checks to see if a server group is associated with the next level of user groups. This process continues until the program finds a user group to which a server group is assigned. When the program finds a server group associated at user group level, it stops to check further. If there are more than one server groups associated at the user group level, then the behavior of the combination of the two server groups (as explained in the above table) is considered. Consider the following scenario to understand server group assignment:

> ### Example
>
> **Scenario:** You schedule document (D).
>
> User (U) belongs to two user groups (UG1 and UG2). But, there is no server group assigned at both UG1 and UG2.
>
> UG1 belongs to User Group 3 (UG3) and UG2 belongs to User Group 4 (UG4).
>
> Server Group 3 (SG3) is set at UG3.
>
> SG3 is set as Required (R).
>
> **Result:** Since there are no server groups set at the first level (UG1 and UG2), the program checks to see if there are any server groups set at the next level (UG3 and UG4). Because SG3 is set at UG3, and SG3 is set as Required, only servers in SG3 are used to process the object and servers from the common pool cannot be used.
>
> This implies that if no server groups are set at the user group level, then the program checks the immediate next level to see if any server groups are set. If the program identifies that a server group is set at any of the user group levels, the program stops checking for server groups at the next level.

- At a document level, there can be only one server group which can be assigned and it can be either Required (R) or Preferred (P). However, a user can belong to one or more user groups and this can result in more than one server group being assigned to a user. If a server group is set at both document (D) and user group (UG) level, then the server group association at document level is always considered over the server group association at user group level. Consider the following scenario to understand server group assignment:

  > ### Example
  >
  > **Scenario:** You schedule document (D).
  >
  > Server Group 1 (SG1) is set at D, and SG1 is set as Required.
  >
  > Server Group 2 (SG2) is set at UG, and SG2 is set as Preferred.
  >
  > **Result:** SG1 is used. As SG1 is set as Required, servers from the common pool cannot be used.
  >
  > Since a server group (SG1) is already set at document (D) level, the program ignores the server group assignment at the user group level. It implies that server group assignment at document level is considered over user group level.

- You need to ensure that all required servers are part of the server group.
- To understand more in detail about server group assignment at folder and user group, read https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

11.8.7 Mapping a Folder to a Server Group

You can now map a folder to a particular server group using the new *Default Settings* option.

Context

To map a folder to a server group, perform the following steps:

Procedure

1. Log on to the CMC.
2. Navigate to *Folders* and right-click on the desired folder (which you want to map the server group to).
3. Select *Default Settings*.
4. In the *Scheduling Server Group* page, set the default servers to use for scheduling at folder-level.

   You can select one of the following options:
   - (Default) Choose *Use the first available server* to run the object on the server with the most resources free at the time of scheduling.
   - Choose *Give preference to servers in the selected group* to run the object on servers in a particular server group. Then select the required server group from the dropdown box to set a preference for a particular server group. If no servers in the selected server group are available, the object is run on the next available server from the common server pool.
   - Choose *Only use servers in the selected group* to run the object only on servers in a particular server group and select the required server group from the dropdown box to exclusively use one server group. If no servers in the selected group are available, the object is not processed.

   > **Note**
   >
   > You can choose to map an exclusive or non-exclusive server group to a folder by selecting one of the two radio buttons: *Give preference to servers in the selected group* or *Only use servers in the selected group*.
   >
   > Similarly, you can assign server groups for viewing or processing Crystal Reports and Web Intelligence documents by navigating to *Default Settings* and *Crystal Reports Process Settings* and *Web Intelligence Process Settings* respectively.
   >
   > If a server group is associated as required, it means that **only** servers from that particular server group are used. Servers from the common pool are not used. If a server group is associated as preferred, then if the servers in the server group are busy, servers from the common server pool are used. Common server pool includes all servers that are not part of any exclusive server group. For more information on exclusive server groups, see To create an exclusive server group [page 421].

5. Choose *Save & Close*.

   You have now successfully mapped a folder to a server group.

Note

- At folder or document level, there can be only one server group which can be assigned and it can be either Required (R) or Preferred (P). If a server group is set at folder (F), document (D), and user group (UG) level, then the server group association at document level is always considered over the server group association at folder level followed by server group association at user group level. Therefore, the order of priority for server group assignment is as follows:
  Document > Folder > User Group
- A document can belong to a folder which can in turn belong to another parent folder. Considering that there is no server group assigned at document level, if no server group is associated with the immediate folder that a document belongs to, then the program checks to see if a server group is associated with the next immediate parent folder. This process continues until the program finds a parent folder to which a server group is assigned. When the program finds a server group associated at folder level, it stops to check further. Consider the following scenario to understand server group assignment:

  #### Example

  Scenario: You schedule document (D).

  But, there is no server group assigned at document level.

  Document (D) belongs to folder (F). But, there is no server group assigned at F.

  Folder (F) is in turn part of another folder: Parent Folder (PF). Server Group (SG) is set at PF.

  SG is set as Required (R).

  Result: Since there are no server groups set at the document (D), the program checks to see if there are any server groups set at the folder level (F). As again there are no server groups set at F, the program checks to see if there are any server groups set at the next level - parent folder (PF). Because SG is set at PF, and SG is set as Required, only servers in SG are used to process the object and servers from the common pool cannot be used.

  This implies that if no server groups are set at the document level, then the program checks the immediate folder to see if any server groups are set. If the program identifies that a server group is set at any of the folder levels, the program stops checking for server groups at the next level.

  Similarly, if there is no server group set at document level, and also no server group set at folder level, then the program considers the server group assignment at user group level
- You need to ensure that all required servers are part of the server group.
- To understand more in detail about server group assignment at folder and user group, read https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

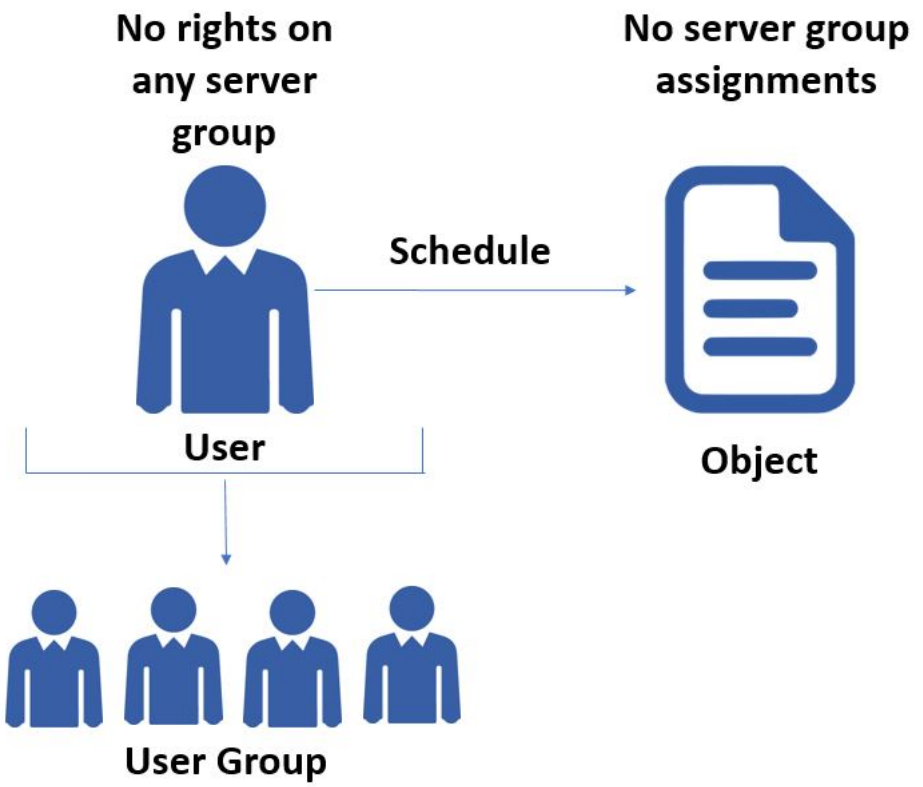
11.8.8 Understanding Server Group Rights Management

You can enable access rights for server groups at the user or user group level. This means that you can control access to the server groups for every user or user group.

> **Note**
>
> - The scenarios mentioned below have used scheduling as a process to explain the server group rights management. Similarly, you can understand the server group rights management for viewing and caching.
> - You can schedule an object successfully if the servers are available in a server group or in a combination of server groups. Scheduling fails if there are no servers available.

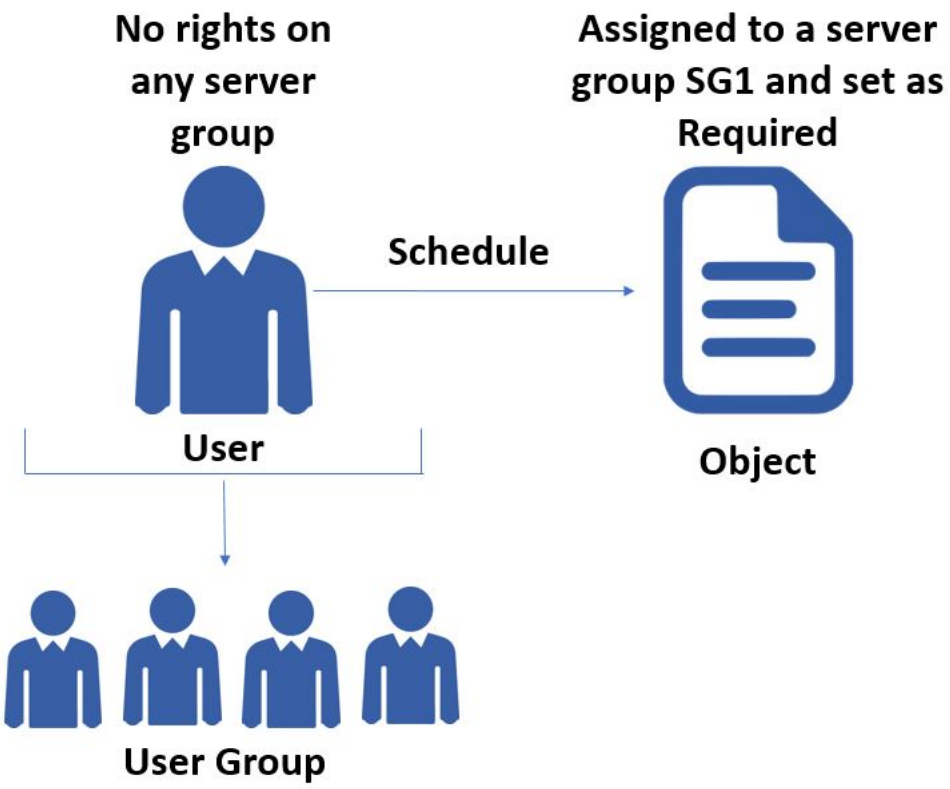
Scenario 1:

Consider an ideal scenario where a user is a part of a user group in the Business Intelligence platform. The user and its associated user group have no rights in any server group. The user now wants to schedule an object that is also not assigned to any server groups.



Scenario 2:

When you modify the above scenario by assigning a server group to the object; scheduling of the object fails.



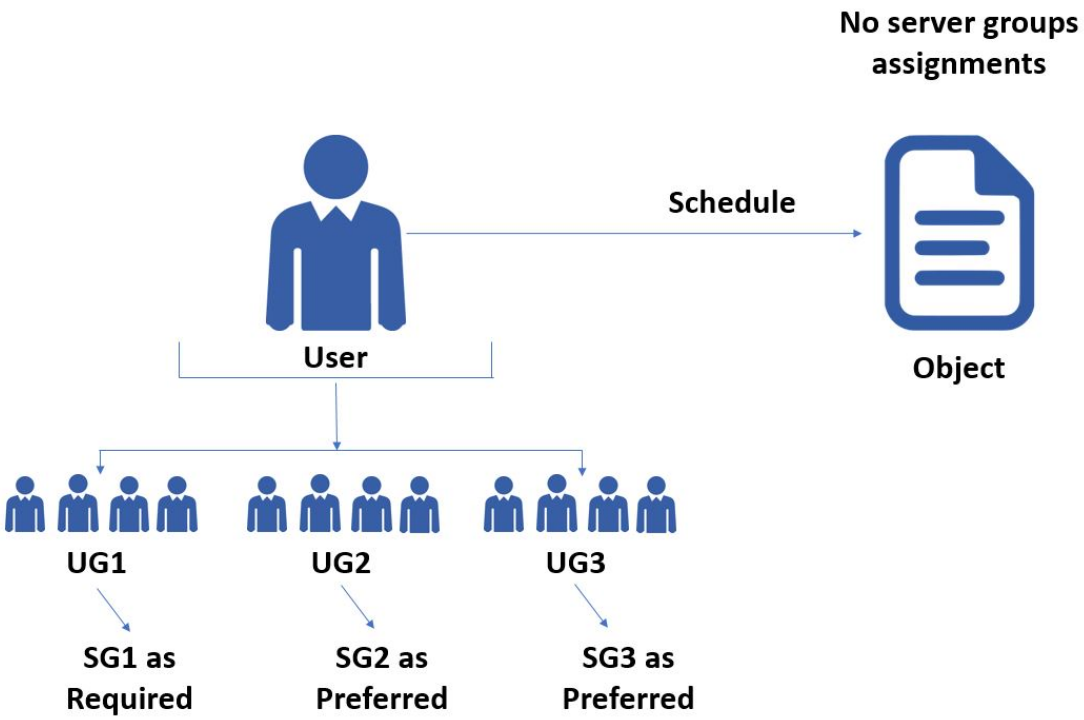
When a user schedules an object, the platform checks for server group assignments to the object. If a server group is assigned to the object, the platform checks whether the user has view rights on the server group.

In the second scenario, neither the user nor his/her associated user group has rights on SG1. This causes the scheduling job to fail. If you want a user to schedule an object successfully in this scenario, ensure that the user or any associated user groups has view rights to SG1.

Scenario 3:

> ⓘ Note
>
> For scenarios 3 and 4, it is assumed that the user inherits the rights from its associated user groups.

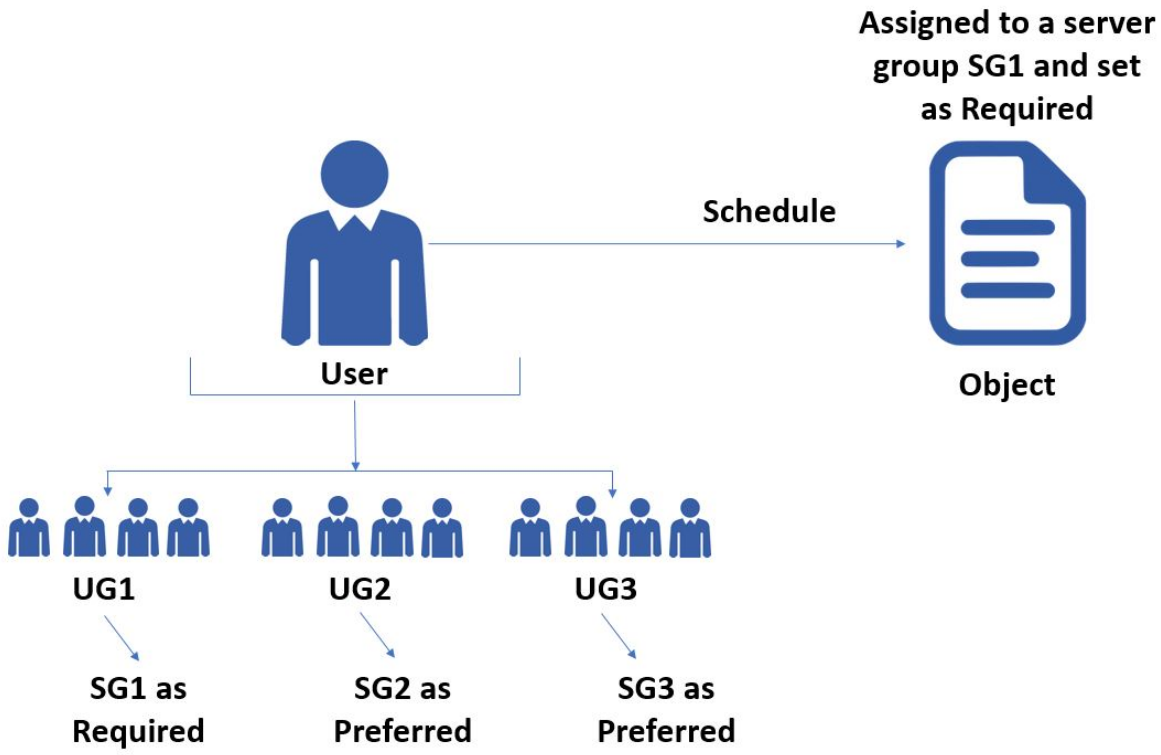
A user is a part of three user groups UG1, UG2, and UG3, and you have mapped each user group to server groups SG1, SG2, and SG3 respectively. SG1 is set as a Required server group however, and SG2 and SG3 are set as Preferred server groups. For more information on how to set a server group as Required or Preferred, see *Mapping a User Group to Server Group* in *Business Intelligence platform Administrator Guide*.



When a user is associated with multiple user groups, and each user group is mapped to a different server group, the platform calculates the available server group. In the above-mentioned scenario, the scheduling job succeeds because the object has no server group assignments, and the available server group to schedule the object is the combination of SG1, SG2, and SG3.

Scenario 4:

In addition to scenario 3, you have assigned the object to SG1 and have set SG1 as Required. For more information on how to set a server group as required or preferred, see *Mapping a User Group to Server Group* in *Business Intelligence platform Administrator Guide*.



When a server group is assigned to an object, the platform checks if you have provided the user with view rights on the server group. In this scenario, the platform doesn't calculate the available server group because a server group assignment at the object level has the highest priority. In scenario 4, the object is scheduled successfully because the UG1 has view rights on SG1, and the user inherits these rights from UG1.

→ Remember

- Before scheduling an object, check the server group assignments to all the user groups associated with the user, and compute the available server group.
- A scheduling job succeeds when the available server group for a user includes the server group assigned to the object.

Refer the table below:

ⓘ Note

Consider SG1 and SG2 is assigned to user groups UG1 and UG2 respectively.

Access Level	Combination of Server Groups (SG1 + SG2)	Searching for servers in Common Pool
User has rights on all server groups	Required + Required	False
User has rights on all server groups	Required + Preferred	False
User has rights on all server groups	Preferred + Preferred	True

Access Level	Combination of Server Groups (SG1 + SG2)	Searching for servers in Common Pool
User has no Rights on any server group	Required + Required	False
User has no Rights on any server group	Required + Preferred	False
User has no Rights on any server group	Preferred + Preferred	True
User has rights on few server groups	Required (No) + Required (Yes)	False
User has rights on few server groups	Required (No) + Preferred (Yes)	False
User has rights on few server groups	Required (Yes) + Preferred (No)	False
User has rights on few server groups	Preferred (No) + Preferred (Yes)	True

11.9 Configuring Adaptive Processing Servers for production systems

The installation program installs one Adaptive Processing Server (APS) per host system. Depending on the features that you've installed, this APS may host a large number of services, such as the Monitoring Service, Promotion Management Service, Multi-Dimensional Analysis Service (MDAS), Publishing Service, and others.

For production or test systems, the best practice is to create additional APSs, and configure the APSs to meet your business requirements.

You can create additional APSs in two ways:

- Run the System Configuration Wizard.
  The wizard helps you with basic configurations of your BI platform system, including configuring APSs according to predefined deployment templates. The APS configuration provided by the wizard is a good starting point; however, system sizing must still be performed.
- Use the CMC to manually create and configure additional APSs.

For more information on configuring adaptive processing servers for production systems, refer the following KBA article at: 1694041.

> → Remember
>
> Selecting a deployment template in the wizard or manually creating additional APSs does not replace system sizing. Ensure that sizing is performed. For more information, refer to How to find sizing information for SAP BI .

11.10 Assessing your system's performance

11.10.1 Monitoring BI platform servers

The Monitoring application provides the ability to capture the runtime and historical metrics of BI platform servers, for reporting and notification. The application helps system administrators to identify if servers are functioning normally and if the response times are as expected.

Related Information

Monitoring [page 727]

11.10.2 Analyzing server metrics

The Central Management Console (CMC) allows you to view the metrics for the servers in your system. These metrics include general information about each machine, along with details that are specific to the type of server. The CMC also allows you to view system metrics, which include information about your product version, your CMS, and your current system activity.

> ⓘ Note
>
> You can only view the metrics for servers that are currently running.

11.10.2.1 To view server metrics

Procedure

1. Go to the *Servers* management area of the CMC.
2. Right-click the server whose metrics you want to view, and select *Metrics*.

Results

The *Metrics* tab displays a list of metrics for the server.

Related Information

To change a server's properties [page 442]
About the Server Metrics Appendix [page 1085]

11.10.3 Viewing system metrics

The *Settings* management area of the CMC displays system metrics that provide general information about your BI platform installation. The *Properties* section includes information about the product version and build. It also lists the data source, database name, and database user name of the CMS database. The *View global system metrics* section lists current account activity, along with statistics about current and processed jobs. The *Cluster* section lists the name of the CMS you are connected to, the name of the CMS cluster, and the names of other cluster members.

11.10.3.1 To view system metrics

Procedure

1. Go to the *Settings* management area of the CMC.
2. Click an arrow to expand and view the settings in the *Properties*, *View Global System Metrics*, *Cluster*, or *Hot Backup* area.

11.10.4 Logging server activity

The BI platform allows you to log specific information about BI platform web activity.

- In addition, each of the BI platform servers is designed to log messages to your operating system's standard system log.
  - On Windows, the BI platform logs to the Event Log service. You can view the results with the Event Viewer (in the Application Log).
  - On UNIX, the BI platform logs to the syslog daemon as a User application. Each server prepends its name and PID to any messages that it logs.

Each server also logs assert messages to the logging directory of your product installation. The programmatic information logged to these files is typically useful only to SAP BusinessObjects support staff for advanced debugging purposes. The location of these log files depends upon your operating system:

- On Windows, the default logging directory is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`.
- On UNIX, the default logging directory `<INSTALLDIR>/sap_bobj/logging` directory of your installation.

The important point to note is that these log files are cleaned up automatically, so there will never be more than approximately 1 MB of logged data per server.

> **Note**
>
> To enable logging to function on UNIX machines that are hosting BI platform servers, you must set up and configure system logging so that all messages logged to the "user" facility of "info" level or higher are recorded. You must also configure `SYSLOGD` to accept remote logging.
>
> Setup procedures vary from system to system. Consult your operating system documentation for specific instructions.

11.11 Configuring server settings

This section includes technical information and procedures that show how you can modify settings for BI platform servers.

The majority of the settings discussed in this section allow you to integrate the BI platform more effectively with your current hardware, software, and network configurations. Consequently, the settings that you choose will depend largely upon your own requirements.

You can change server settings though the Central Management Console (CMC) in two ways.

- On the *Properties* screen for the server.
- On the *Edit Common Services* screen for the server.

It is important to note that not all changes occur immediately. If a setting cannot change immediately, the *Properties* and *Edit Common Services* screens display both the current setting (in red text) and the desired setting. When you return to the Servers management area, the server will be marked as Stale. When you restart the server, it will use the desired settings and the Stale flag is removed from the server.

> **Note**
>
> This section does not show how to configure your Web application server to deploy BI platform applications. This task is typically performed when you install the product. For details, see the *SAP BusinessObjects Business Intelligence platform Installation Guide*.

Related Information

Configuring port numbers [page 451]
To change a server's properties [page 442]
Recreating the CMS system database [page 493]
Selecting a new or existing CMS database [page 490]

11.11.1 To change a server's properties

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the server whose settings you want to change.
   The *Properties* screen appears.
3. Make the changes you want, then click *Save* or *Save & Close*.

> **Note**
>
> Not all changes occur immediately. If a setting cannot change immediately, the Properties dialog box display both the current setting (in red text) and the desired setting. When you return to the Servers management area, the server will be marked as Stale. When you restart the server, it will use the desired settings from the Properties dialog box and the Stale flag is removed from the server.

11.11.2 To apply service settings to multiple servers

Context

You can apply the same setting to services that are hosted on multiple servers.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Pressing `Ctrl`, click each server that hosts services for which you want to change settings, and then right-click and select *Edit Common Services*.
   The *Edit Common Services* dialog box appears, displaying a list of services hosted on the servers you selected that have settings you can change.
3. If the *Edit Common Services* dialog box lists more than one service, select the service you want to edit, and click *Continue*.
4. Make changes as needed, and click *OK*.

Results

> **Note**
>
> You are redirected to the *Servers* management area of the CMC. If a server requires a restart, the server is marked as Stale. When you restart the server, it uses the new settings and the Stale flag is removed.

11.11.3 Working with configuration templates

Configuration templates allow you to easily configure multiple instances of servers. Configuration templates store a list of settings for each service type, which you can use to configure additional server instances. For example, if you have a dozen Web Intelligence Processing Servers that you want to configure identically, you only need to configure settings for one of them. You can then use the configured service to define the configuration template for Web Intelligence Processing Servers, and then apply the template to the other 11 service instances.

Each type of BI platform service has its own configuration template. For example, there is one configuration template for the Web Intelligence Processing service type, one for the Publishing service type, and so on. The configuration template is defined in the server properties in the Central Management Console (CMC).

When you make a server use a configuration template, existing settings for the server are overwritten with the values from the template. If you later decide to stop using the template, the original settings are not restored. Subsequent changes to the configuration template no longer affect the server.

It is good practice to use configuration templates as follows:

1. Set the configuration template on one server.
2. Assuming you want the same configuration on all servers of the same type, check *Use Configuration Template* for all servers of the same type, including the one where you set the configuration template.
3. Later, if you want to change the configuration of all services of this type, view the properties of any one of the services, deselect the *Use Configuration Template* check box. Change the settings you want, then select *Set Configuration Template* for this server and click *Save*. All services of that type are updated. By not having a server that is always set as the configuration template, you ensure that you will not accidentally change configuration settings for all servers of that type.

Related Information

To set a configuration template [page 443]
To apply a configuration template to a server [page 444]

11.11.3.1 To set a configuration template

Context

You can set a configuration template for each type of service. You cannot set multiple configuration templates for a service. You can use any server's *Properties* page to configure the settings that will be used by the configuration template for a service type that is hosted on the server.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the server that hosts services whose configuration template you want to set.
   The *Properties* screen appears.
3. Configure the service settings that you want to use in the template, select the *Set Configuration Template* check box and click *Save* or *Save & Close*.

Results

The configuration template for the service type that you selected is defined according to the settings of the current server. Other servers of the same type hosting the same services will be automatically and immediately reconfigured to match the configuration template if they have the *Use Configuration Template* option enabled in their properties.

> **Note**
>
> If you don't explicitly define the settings for the configuration template, the service's default settings are used.

Related Information

To apply a configuration template to a server [page 444]

11.11.3.2 To apply a configuration template to a server

Context

Before you apply a configuration template, ensure that you have defined the configuration template settings for the type of server you want to apply the template to. If you haven't explicitly defined the configuration template settings, the default settings for the service are used.

> **Note**
>
> Servers that do not have the Use Configuration Template setting enabled will not be updated when you modify the settings of the configuration template.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the server that is hosting a service you want to apply the configuration template to.
   The *Properties* screen appears.
3. Select the *Use Configuration Template* check box and click *Save* or *Save & Close*.

> **Note**
>
> If the server requires you to restart it in order for the new settings to take effect, it will show up as "stale" in the servers list.

Results

The appropriate configuration template is applied to the current server. Any subsequent changes to the configuration template change the configuration of all servers that use the configuration template.

Unchecking *Use Configuration Template* does not restore the server configuration to the values as they were when the configuration template was applied. Subsequent changes to the configuration template do not affect the configuration of the servers that are using the configuration template.

Related Information

To set a configuration template [page 443]

11.11.3.3 To restore system defaults

Context

You may want to restore a service's configuration to the settings it was initially installed with (for example, if you misconfigure the servers, or experience performance issues).

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the server hosting a service that you want to restore system defaults for.
   The *Properties* screen appears.
3. Select the *Restore System Defaults* check box and click *Save* or *Save & Close*.

The default settings for the particular service type are restored.

11.12 Configuring server network settings

The networking settings for BI platform servers are managed through the CMC. These settings are divided into two categories: port settings and host identification.

Default settings

During installation, server host identifiers are set to *Auto assign*. Each server can however be assigned either a specific IP address or a hostname. The default CMS port number is 6400. The other BI platform servers dynamically bind to available ports. Port numbers are automatically managed by the BI platform, but you can use the CMC to specify port numbers.

11.12.1 Network environment options

The BI platform supports Internet Protocol version 4 (IPv4) and Mixed IPv4/IPv6 network traffic. You can use the server and client components in any of the following environments:

- IPv4 network: all server and client components run with IPv4 protocol only.
- Mixed IPv6/IPv4 network: server and client components can run with both IPv6 and IPv4 protocols. i.e.
  - IPv6-only (IPv6 stack enabled, IPv4 stack installed and IPv4 stack disabled)
  - IPv6/IPv4 mixed (both IPv6 stack and IPv4 stack enabled)
  - IPv4 only (IPv4 stack enabled, IPv6 stack disabled or uninstalled) hosts.

> **Note**
>
> - Network configuration should be performed by the system and network administrator. The BI platform does not provide a mechanism to designate a networking environment. You can use the CMC to bind to a specific IPv6 or IPv4 address for any of your BI platform servers.
> - Pure IPv6 stack (IPV6 alone installed and enabled) is not supported. However, Mixed IPv6 network is supported.

11.12.1.1 Mixed IPv6/IPv4 environment

The IPv6/IPv4 networking environment enables the following:

- BI platform servers can service both IPv6 and IPv4 requests when running in mixed IPv6/IPv4 mode.

- Client components can interoperate with servers as IPv4-only nodes, or IPv6/IPv4 nodes.

The mixed mode is particularly useful in the following scenarios:

- You are moving from an IPv4-only node to a Mixed IPv6 node environment. All the client and server components will continue to seamlessly interoperate until the transition is complete. You can then deactivate the IPv4 settings for all the servers.
- Third party software that is not IPv6 compatible will continue to function in the IPv6/IPv4 node environment.

11.12.2 Server host identification options

Host identification options can be specified in the CMC for all BI platform servers. The following table summarizes the options available in the *Common Settings* area:

Option	Description
Auto assign	This is the default setting for all servers. When this check box is selected, the server automatically binds the server's request port onto the first network interface on the machine. **Note** It is good practice to select the *Auto assign* check box for the host name. However, in some cases, such as when the server is running on multi-homed machine, or when the server needs to inter-operate with a certain firewall configuration, you should consider using either a specific hostname or IP address. See the information about configuring a multihomed machine and working with firewalls in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
Hostname	Specifies the host name of the network interface that the server listens for requests on. For the CMS, this setting specifies the host name of the network interface that the CMS binds the name server port and the request port.
IP Address	Specifies the IP address of the network interface that the server listens for requests on. For the CMS, it specifies the address of the network interface that the CMS uses to bind the name server port to the request port. For all servers, separate fields are provided to specify IPv4 and/or IPv6 IP addresses.

Caution

If you select the *Auto assign* check box on a multi-homed machine, the CMS may automatically bind to the wrong network interface. To avoid this, make sure the network interfaces on the host machine are listed

in the correct order (using the machine's operating system tools). You must specify the host name for the CMS in the CMC.

> **Note**
>
> If you are working with multi-homed machines or in some NAT firewall configurations, you may need to specify the host name using fully qualified domain names instead of host names.

Related Information

To configure the system for firewalls [page 197]
Configuring a multi-homed machine [page 449]
To troubleshoot multiple network interfaces [page 450]

11.12.2.1 To modify a server's host identification

Procedure

1. Go to the *Servers* management area of the CMC.
2. Select the server, then choose *Stop Server* from the *Actions* menu.
3. Choose *Properties* from the *Manage* menu.
4. Under *Common Settings*, select one of the following options:

Option	Description
Auto assign	The server will bind to one of the available network interfaces.
Hostname	Enter the host name of the network interface on which server listens for requests.
IP Address	Enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface on which server listens for requests. **Note** To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

5. Click *Save* or *Save & Close*.
   The changes are reflected in the command line displayed on the *Properties* tab.
6. Start and enable the server.

11.12.3 Configuring a multi-homed machine

A multi-homed machine is one that has multiple network addresses. You may accomplish this with multiple network interfaces, each with one or more IP addresses, or with a single network interface that has been assigned multiple IP addresses.

If you have multiple network interfaces, each with a single IP address, change the binding order so that the network interface at the top of the binding order is the one you want the BI platform servers to bind to. If your interface has multiple IP addresses, use the Host Identifiers option in the CMC to specify a network interface card for the BI platform server. It can be specified by host name or IP address. For more information about configuring the *Host Identifiers* setting, see "To troubleshoot multiple network interfaces".

> → Tip
>
> This section shows how to restrict all servers to the same network address, but it is possible to bind individual servers to different addresses. For instance, you might want to bind the File Repository Servers to a private address that is not routable from users' machines. Advanced configurations such as this require your DNS configuration to route communications effectively between all the BI platform server components. In this example, the DNS must route communications from the other BI platform servers to the private address of the File Repository Servers.

Related Information

To troubleshoot multiple network interfaces [page 450]

11.12.3.1 To configure the CMS to bind to a network address

Context

> ⓘ Note
>
> On a multi-homed machine, the Host Identifier can be set to the fully qualified domain name or the IP address of the interface that you want the server to bind to.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the CMS.
3. Under *Common Settings*, select one of the following options:
   - *Hostname*

- Enter the host name of the network interface to which the server will bind.
- *IP Address*
- Enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface to which the server will bind.

  > **Note**
  >
  > To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

> **Caution**
>
> Do not select Auto assign.

4. For *Request Port* you can do one of the following:
   - Select the *Auto assign* option.
   - Enter a valid port number in the *Request Port* field.
5. Make sure that a port number is specified in the Name Server Port dialog box.

> **Note**
>
> The default port number is 6400.

11.12.3.2 Configuring the remaining servers to bind to a network address

The remaining BI platform servers select their ports dynamically by default. For information on disabling the Auto assign setting that dynamically propagates this information, see “To change the port a server uses for accepting requests ”.

Related Information

To change the port a server uses for accepting requests [page 454]

11.12.3.3 To troubleshoot multiple network interfaces

Context

On a multi-homed machine, the CMS may automatically bind to the wrong network interface. To prevent this from happening, you can ensure the network interfaces on the host machine are listed in the correct order (using the machine's OS tools), or make sure you specify the Host Name setting for the CMS in the CMC. If the primary network interface is not routable, you can use the following procedure to configure the BI platform

to bind to a non-primary routable network interface. Perform these steps immediately after installing the BI platform on the local machine, before you install the BI platform on other machines.

Procedure

1. Open the CCM and stop the SIA for the node on the machine that has multiple network interfaces.
2. Right-click the SIA and choose *Properties*.
3. In the *Properties* dialog box, click the *Configuration* tab.
4. To bind the SIA to a specific network interface, type the port number of the target network interface in the *Port* field.
5. Click *OK* and select the *Startup* tab.
6. From the *Local CMS Servers* list select the CMS and click *Properties.*
7. To bind the CMS to a specific network interface, type the port number of the target network interface in the *Port* field.
8. Click *OK* to apply the new settings.
9. Start the SIA and wait for the servers to start.
10. Launch the Central Management Console (CMC), and go to the *Servers* management area. Repeat steps 11-14 for each server.
11. Select the server, then choose *Stop Server* from the *Actions* menu.
12. Choose *Properties* from the *Manage* menu.
13. Under *Common Settings*, select one of the following options:
    - Hostname: enter the host name of the network interface to which the server will bind.
    - IP Address: enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface to which the server will bind.

      > **Note**
      >
      > To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

    > **Caution**
    >
    > Do not select Auto assign.
14. Click *Save* or *Save & Close*.
15. Return to the CCM and restart the SIA.

    The SIA restarts all servers on the node. All servers on the machine now bind to the correct network interface.

11.12.4 Configuring port numbers

During installation, the CMS is set up to use default port numbers. The default CMS port number is 6400. This port falls within the range of ports reserved by SAP BusinessObjects (6400 to 6410). Communication on these ports should not conflict with third-party applications.

When started and enabled, each of the other BI platform servers dynamically binds to an available port (higher than 1024), registers with this port on the CMS, and then listens for BI platform requests. If necessary, you can instruct each server component to listen on a specific port (rather than dynamically selecting any available port). For example, you will need to manually configure a request port for each BI platform server that must communicate across a firewall.

Port numbers can be specified on each server's Properties tab in the CMC. This table summarizes the options under the *Common Settings* area as they relate to port usage for specific server types:

Setting	CMS	Other Servers
Request Port	Specifies the port that the CMS uses for accepting all requests from other servers (except for Name Server requests). Uses the same network interface as the Name Server Port. When *Auto assign* is selected, the server automatically uses an OS-assigned port number.	Specifies the port on which the server listens for all requests. When *Auto assign* is selected, the server automatically uses a port number assigned by the OS.
Name Server Port	Specifies the BI platform port on which the CMS listens for name service requests. The default is 6400.	Not applicable.

11.12.4.1 To change the default CMS port in the CMC

Context

If there is a CMS already running on the cluster, you can use the CMC to change the default CMS port number. If no CMS is running on the cluster, you must use the CCM on Windows, or the `serverconfig.sh` script on UNIX, to change the port number.

> **Note**
>
> The CMS uses the same network interface card for the request port and the name server port.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Double-click the CMS in the server list.
3. Replace the *Name Server Port* number with the port that you want the CMS to listen on. (The default port is 6400.)
4. Click *Save & Close*.
5. Restart the CMS.

   The CMS begins listening on the port number you specified. The Server Intelligence Agent dynamically propagates the new settings to the other servers on the node, if those servers have the *Auto assign* option

selected for the request port. (It may take several minutes for your changes to appear in the Properties settings of all node members.)

The settings you choose on the *Properties* page are reflected in the server command line, which also appears on the *Properties* page.

11.12.4.2 To change the default CMS port in the CCM on Windows

Context

If no CMS is accessible on the cluster and you want to modify the default CMS port for one or more CMSs in your deployment, you must use the CCM to change the CMS port number.

Procedure

1. Open the CCM and stop the SIA for the node.
2. Right-click the SIA and choose *Properties*.
3. In the *Properties* dialog box, click the *Startup* tab.
4. From the *Local CMS Servers* list select the CMS that you want to change the port number for, and click *Properties*.
5. To bind the CMS to a specific port, type the port number in the *Port* field.
6. Click *OK* to apply the new settings.
7. Start the SIA and wait for the servers to start.

11.12.4.3 To change the default CMS port in the CCM on Unix

Context

If no CMS is accessible on the cluster and you want to modify the default CMS port for one or more CMSs in your deployment, use the `serverconfig.sh` script to change the CMS port number.

Procedure

1. Use the `ccm.sh` script to stop the Server Intelligence Agent (SIA) that hosts the CMS whose port number you want to change.
2. Run the `serverconfig.sh` script.

By default this script is in the `<InstallDir>/sap_bobj` directory.

3. Select *3 - Modify node*, and press `Enter`.
4. Select the node that hosts the CMS that you want to modify, and press `Enter`.
5. Select *3 - Modify a local CMS*, and press `Enter`.
   A list of CMSs hosted on the node appears.
6. Select the CMS to modify, and press `Enter`.
7. Type the new port number for the CMS, and press `Enter`.
8. Specify whether you want the CMS to automatically start when the SIA starts, and press `Enter`.
9. Type the command-line arguments for the CMS or accept the current arguments, and press `Enter`.
10. Type **`quit`** to exit the script.
11. Start the SIA with the `ccm.sh` script, and wait for the servers to start.

11.12.4.4 To change the port a CMS uses for accepting requests

Procedure

1. Go to the *Servers* management area of the CMC.
2. Select the CMS, then choose *Properties* from the *Manage* menu.
3. Under *Common Settings*, deselect the *Auto assign* check box for *Request Port*, then type the port number you want the server to listen on.
4. Click *Save* or *Save & Close*.
5. Restart the CMS.

Results

The CMS binds to the new port, and starts listening for requests from other servers.

11.12.4.5 To change the port a server uses for accepting requests

Context

> **Note**
>
> These steps cannot be used to change the request port for the Central Management Server (CMS). See “To change the port a CMS uses for accepting requests” instead.

Procedure

1. Go to the *Servers* management area of the CMC.
2. Select the server, then choose *Stop Server* from the *Actions* menu.
3. Double-click the server.
   The *Properties* screen appears.
4. Under *Common Settings*, deselect the *Auto assign* check box for *Request Port*, then type the port number you want the server to listen on.
5. Click *Save* or *Save & Close*.
6. Start and enable the server.

Results

The server binds to the new port, registers with the CMS, and begins listening for BI platform requests on the new port.

11.13 Managing Nodes

11.13.1 Using nodes

A node is a group of BI platform servers that run on the same host and are managed by the same Server Intelligence Agent (SIA). All servers on a node run under the same user account. One machine can contain many nodes so you can run processes under different user accounts. One SIA manages and monitors all servers on a node, ensuring they operate properly.

> ⓘ Note
>
> You must use an Administrator account with Enterprise authentication to perform all node management procedures securely. However, if SSL communication between servers is enabled, you must disable SSL before you can perform node management tasks.

> ⓘ Note
>
> Ensure that all database drivers needed for any BI platform servers to connect to their datasources (for example, for the CMS to connect to the CMS database) are present, and that the correct environment has already been set up (for example, appropriate environment variables have been set).

11.13.1.1 Variables

Variable	Description
<INSTALLDIR>	The directory where SAP BusinessObjects Business Intelligence platform is installed. On Windows: `C:\Program Files (x86)\SAP BusinessObjects`
<SCRIPTDIR>	The directory where node management scripts are located. • On Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts • On Unix: <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts
<PLATFORM32>	The name of your Unix operating system. Acceptable values are: • linux_x86 • win32_x86
<PLATFORM64>	The name of your Unix operating system. Acceptable values are: • linux_x64 • win64_x64

11.13.1.2 To prepare a Unix machine for SQL Anywhere

Context

You must create an `odbc.ini` file and source it before you can use SQL Anywhere as an ODBC data source on a Unix machine.

> **Note**
>
> This procedure is unnecessary if you use the bundled SQL Anywhere installed with the BI platform.

Procedure

1. Create `odbc.ini` in <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>.
2. Enter the database source name (DSN), the database name and server name for SQL Anywhere, and the IP address and port number of the machine that hosts the SQL Anywhere database server.

3. Save `odbc.ini`.
4. Bring the SQL Anywhere environment into your current environment.

   For example, if you are using Bash as your command line shell, source the 64-bit version of `sa_config.sh`.
5. Define an environment variable named `ODBCINI` that points to where the `odbc.ini` file was created.

   Set up that environment variable so that child processes can see the `ODBCINI` environment variable.

Example

A sample `odbc.ini` file:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0
[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

A sample `source` command:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

Related Information

Variables [page 456]

11.13.2 Adding a new node

The installation program creates a single node when you first install the BI platform.

You may need additional nodes if you want to run servers under different user accounts.

You can add a new node using the Central Configuration Manager (CCM), or using a node management script. If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

> ⓘ Note
>
> Use the CCM or node management script on the machine where you want to add a node. It is not possible to add a node on a remote machine.

A BI platform installation is a unique instance of the BI platform files created by the installer on a machine. An instance of a BI platform installation can be used only within a single cluster. Nodes belonging to different

clusters sharing the same BI platform installation are not supported because this type of deployment cannot be patched or updated. Only Unix platforms support multiple installations of the software on the same machine, and only if each installation is performed under a unique user account and is installed to a separate folder so that the installations do not share any files.

Remember that all machines in the cluster must have the same version and patch level.

→ Recommendation

To add nodes to a BI platform deployment in which FIPS is enabled and CORBA SSL is configured, it is recommended that you use the "Start a new temporary CMS" option.

To add nodes to a BI platform deployment in which FIPS is not enabled and CORBA SSL is configured, it is recommended that you use the "Start a new temporary CMS" option.

To add nodes to a BI platform deployment in which FIPS is enabled and CORBA SSL is not configured, it is recommended that you use the existing CMS.

11.13.2.1 Adding a node to a new machine on an existing deployment

You can automatically create the first node on a machine when you use the installation program to add a new machine to an existing deployment.

→ Tip

During the installation, click *Expand*, and specify your existing Central Management Server.

If you want to create additional nodes, use the Central Configuration Manager or the `serverconfig.sh` script.

For more information on installation, see the *SAP BI platform Installation Guide*.

11.13.2.2 To add a node on Windows

Context

⚠ Caution

Back up the server configuration for the entire cluster before and after you add a node.

Procedure

1. In the Central Configuration Manager (CCM), on the toolbar, click *Add Node*.

2. In the *Add Node Wizard*, enter the node name and port number for the new Server Intelligence Agent (SIA).
3. Choose whether you want to create servers on the new node.
   - *Add node with no servers*
   - *Add node with CMS*
   - *Add node with default servers*
     This option creates only the servers installed on this machine. It does not include all possible servers.
4. Select a CMS.
   - If your deployment is running, select *Use existing running CMS*, and click *Next*.
     If prompted, enter the host name and port number for the existing CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key.
   - If your deployment is stopped, select *Start a new temporary CMS*, and click *Next*.
     If prompted, enter the host name and port number for the temporary CMS, the Administrator credentials, the data source name, the database credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > ⚠ Caution
     >
     > Avoid using the deployment while the temporary CMS runs. Ensure that the existing and new CMS use different ports.
5. Review the confirmation page, and click *Finish*.
   The CCM creates a node. If any errors occur, review the log file.

Next Steps

You can now use the CCM to start the new node.

11.13.2.2.1 Adding a node on Windows using a script

> ⚠ Caution
>
> Back up the server configuration for the entire cluster before and after you add a node.

You can use `AddNode.bat` to add a node on a Windows machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in these parameters, unless you enclose the text within quotation marks.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
```

```
  -siaport 6415
      -cms mycms:6400
      -username Administrator
      -password My^ Password
      -cmsport 7400
      -dbdriver mysqldatabasesubsystem
      -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
      -dbkey abc1234
      -noservers
      -createcms
```

> **Note**
>
> To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

Related Information

Variables [page 456]
Script parameters for adding, recreating, and deleting nodes [page 475]

11.13.2.3 To add a node on Unix

Context

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you add a node.

Procedure

1. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
2. Select *1 - Add node*, and press `Enter`.
3. Type the name of the new node, and press `Enter`.
4. Type the port number of the new SIA, and press `Enter`.
5. Choose whether you want to create servers on the new node.
   - *no servers*
     Creates a node that does not contain any servers.
   - *cms*
     Creates a CMS on the node, but does not create other servers.
   - *default servers*

Creates only the servers installed on this machine. It does not include all possible servers.

6. Select a CMS.
   - If your deployment is running, select *existing*, and press Enter.
     If prompted, enter the host name and port number for the existing CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key.
   - If your deployment is stopped, select *temporary*, and press Enter.
     If prompted, enter the host name and port number for the temporary CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > ⚠ Caution
     >
     > Avoid using the deployment while the temporary CMS runs. Ensure that the existing and new CMS use different ports.

7. Review the confirmation page, and press Enter.
   The CCM creates a node. If any errors occur, review the log file.

Next Steps

You can now run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the new node.

11.13.2.3.1 Adding a node on Unix using a script

> ⚠ Caution
>
> Back up the server configuration for the entire cluster before and after you add a node.

You can use `addnode.sh` to add a node on a Unix machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
  -createcms
```

Related Information

Variables [page 456]
Script parameters for adding, recreating, and deleting nodes [page 475]

11.13.3 Recreating a node

You can recreate a node using the Central Configuration Manager (CCM), or using a node management script, after you restore the server configuration for the entire cluster, or if the machine hosting your deployment fails, becomes damaged, or has a corrupt file system. Use the following guidelines:

- It is not necessary to recreate a node if you reinstall the deployment on a replacement machine with identical installation options and node name. The installation program automatically recreates the node.
- A node should be recreated only on a machine with an existing deployment with identical installation options and patch level.
- You should recreate only nodes that do not exist on any machines in your deployment. Ensure that no other machines host the same node.
- Although the deployment allows nodes to run on different operating systems, you should recreate nodes only on machines that use the same operating system.
- If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

> ⓘ Note
>
> All servers except the CMS should be stopped before you can recreate a node

> → Remember
>
> You can recreate a node only on the machine where the node is located.

11.13.3.1 To recreate a node on Windows

Procedure

1. In the Central Configuration Manager (CCM), on the toolbar, click *Add Node*.
2. In the *Add Node Wizard*, enter the node name and port number for the recreated Server Intelligence Agent (SIA).

   > ⓘ Note
   >
   > The names of the original and recreated nodes must be identical.
3. Select *Recreate node*, and click *Next*.

- If the node exists in the system database of the Central Management Server (CMS), it is recreated on the local host.

  > ⚠ Caution
  >
  > Use this option only if the node does not exist on any hosts in the cluster.

- If the node does not exist in the system database of the CMS, a new node with default servers is added. Default servers include all of the servers installed on the host.

4. Select a CMS.
   - If your CMS is running, select *Use existing running CMS*, and click *Next*.
     If prompted, enter the host name and port number for the existing CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key.
   - If your CMS is stopped, select *Start a new temporary CMS*, and click *Next*.
     If prompted, enter the host name for the temporary CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > ⚠ Caution
     >
     > Avoid using the deployment while the temporary CMS runs.

5. Review the confirmation page, and click *Finish*.
   The CCM recreates the node, and adds information about the node to the local machine. If any errors occur, review the log file.

Next Steps

You can now use the CCM to start the recreated node.

11.13.3.1.1 Recreating a node on Windows using a script

You can use `AddNode.bat` to recreate a node on a Windows machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in these parameters, unless you enclose the text within quotation marks.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
  -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
```

```
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
  -adopt
```

> **Note**
>
> To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

Related Information

Variables [page 456]
Script parameters for adding, recreating, and deleting nodes [page 475]

11.13.3.2 To recreate a node on Unix

Procedure

1. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
2. Select *1 - Add node*, and press `Enter`.
3. Type the name of the new node, and press `Enter`.

   > **Note**
   >
   > The names of the original and recreated nodes must be identical.
4. Type the port number of the new SIA, and press `Enter`.
5. Select *recreate node* and press `Enter`.
   - If the node exists in the system database of the Central Management Server (CMS), it is recreated on the local host.

     > **Caution**
     >
     > Use this option only if the node does not exist on any hosts in the cluster.
   - If the node does not exist in the system database of the CMS, a new node with default servers is added. Default servers include all of the servers installed on the host.
6. Select a CMS.
   - If your deployment is running, select *existing*, and press `Enter`.
     If prompted, enter the host name and port number for the existing CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key.
   - If your deployment is stopped, select *temporary*, and press `Enter`.

If prompted, enter the host name for the temporary CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

> ⚠ Caution
>
> Avoid using the deployment while the temporary CMS runs.

7. Review the confirmation page, and press `Enter`.
   The CCM recreates the node, and adds information about the node to the local machine. If any errors occur, review the log file.

Next Steps

You can now run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the recreated node.

11.13.3.2.1 Recreating a node on Unix using a script

You can use `addnode.sh` to recreate a node on a Unix machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

Related Information

Variables [page 456]
Script parameters for adding, recreating, and deleting nodes [page 475]

11.13.4 Deleting a node

You can delete a stopped node using a running Central Configuration Manager (CCM), or using a node management script. Use the following guidelines:

- Deleting a node also permanently deletes the servers on the node.
- If your cluster has multiple machines, delete the nodes before you remove a machine from the cluster and uninstall the software from it. If you remove a machine from a cluster before deleting a node, or if the file system on a machine malfunctions, you must recreate the node on a different machine with the same servers, in the same cluster, and then delete the node.

> → Remember
>
> You can delete a node only on the machine where the node is located.

Related Information

Recreating a node [page 462]

11.13.4.1 To delete a node on Windows

Context

> ⚠ Caution
>
> Back up the server configuration for the entire cluster before and after you delete a node.

Procedure

1. Run the Central Configuration Manager (CCM).
2. In the CCM, stop the node that you want to delete.
3. Select the node, and click *Delete Node* on the toolbar.
4. If prompted, enter the host name, port, and Administrator credentials for the CMS.

Results

The CCM deletes the node and all the servers on the node.

> **Note**
>
> You can delete a newly added node after configuring SSL using the following two ways:
>
> - Remove SSL parameters from both the newly created node and the SIA node whose CMSes you are trying to connect.
> - Add the following SSL parameters to RemoveNode.bat before the main class declaration and run it: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.1.1 Deleting a node on Windows using a script

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you delete a node.

You can use `RemoveNode.bat` to delete a node on a Windows machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Related Information

Variables [page 456]
Script parameters for adding, recreating, and deleting nodes [page 475]

11.13.4.2 To delete a node on Unix

Prerequisites

Before and after you delete a node, back up the server configuration for the entire cluster.

Procedure

1. Run `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>` to stop the node that you want to delete.
2. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
3. Select *2 - Delete node*, and press `Enter`.
4. Select the node you want to delete, and press `Enter`.
5. If prompted, enter the host name, port number, and Administrator credentials for the CMS.

Results

The node and all the servers on the node are deleted.

> **Note**
>
> You can delete a newly added node after configuring SSL using the following two ways:
>
> - Remove SSL parameters from both the newly created node and the SIA node whose CMSes you are trying to connect.
> - Add the following SSL parameters to RemoveNode.bat before the main class declaration and run it: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.2.1 Deleting a node on Unix using a script

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you delete a node.

You can use `removenode.sh` to delete a node on a Unix machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

Example

```
<SCRIPTDIR>\removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Related Information

Variables [page 456]
Script parameters for adding, recreating, and deleting nodes [page 475]

11.13.5 Renaming a node

You can rename a node using the Central Configuration Manager (CCM). In order to rename a node, you must create a new node with a new name, clone the servers from the original node to the new node, and then delete the original node. Use the following guidelines:

- If you rename the machine where a node is located, you do not need to rename the node. You can continue to use the existing node name.
- If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

> → Remember
>
> You can rename a node only on the machine where the node is located.

Related Information

Adding a new node [page 457]
Deleting a node [page 466]

11.13.5.1 To rename a node on Windows

Context

> ⚠ Caution
>
> Back up the server configuration for the entire cluster before and after you rename a node.

Procedure

1. Start the Central Configuration Manager (CCM).
2. In the Central Configuration Manager (CCM), on the toolbar, click *Add Node*.

3. In the *Add Node Wizard*, enter the node name and port number for the new Server Intelligence Agent (SIA), the Administrator credentials, the database connection information, the credentials for the system database, and the cluster key.
4. Select *Add node with no servers*.
5. After the node is created, use the *Server Management* page of the Central Management Console to clone all of the servers from the original node to the new node.

   > **Note**
   >
   > Ensure that the cloned servers have no port conflicts with servers on the old node.

6. In the CCM, start the new node.
7. After the new node has been running for five minutes, use the CCM to delete the original node.

Related Information

Adding a new node [page 457]
Deleting a node [page 466]

11.13.5.2 To rename a node on Unix

Context

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you rename a node.

Procedure

1. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`.
2. Select *1 - Add node*, and press `Enter`.
3. Type the name of the new node, and press `Enter`.
4. Type the port number of the new SIA, and press `Enter`.
5. If prompted, enter the Administrator credentials, the database connection information, the credentials for the system database, and the cluster key.
6. Select *no servers* and press `Enter.`
7. After the node is created, use the *Server Management* page of the Central Management Console to clone all of the servers from the original node to the new node.

> **Note**
>
> Ensure that the cloned servers have no port conflicts with servers on the old node.

8. Run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the new node.
9. After the new node has been running for five minutes, use `serverconfig.sh` to delete the original node.

Related Information

Adding a new node [page 457]
Cloning servers [page 412]
Deleting a node [page 466]

11.13.6 Moving a node

You can move a stopped node from one cluster to another using the Central Configuration Manager (CCM), or using a node management script. Use the following guidelines:

- Ensure that the destination cluster does not have a node with the same name.
- Ensure that all server types installed on the machine where the source node is located are also installed on the destination cluster.
- If you want to add a new machine to a production cluster but do not want the machine to be usable until you finish testing it, install the BI platform on a stand-alone machine, test the machine, then move the node to a production cluster.
- The BI platform version and service pack level for this machine must be consistent with the rest of the cluster.

> **→ Remember**
>
> You can move a node only on the machine where the node is located.

11.13.6.1 To move an existing node on Windows

Context

In this example, the node that you want to move is installed on the source system. The source system machine was initially standalone, but it will be added to the destination cluster.

> **⚠ Caution**
>
> Back up the server configuration for the entire cluster before and after you move a node.

Procedure

1. Stop the node in the Central Configuration Manager (CCM).
2. Right-click the node and select *Move*.
3. If prompted, select the data source name, and enter the host name, the port, the database connection information, the Administrator credentials for the destination CMS, and the cluster key.
4. Select a CMS.
   - If your source deployment is running, select *Use existing running CMS*, and click *Next*.
     If prompted, enter the host name and port number for the source system's existing CMS and the Administrator credentials.
   - If your source deployment is stopped, select *Start a new temporary CMS*, and click *Next*.
     If prompted, enter the host name and port number for the source system's temporary CMS, the Administrator credentials, the data source name, the database credentials for the source system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > ⚠ Caution
     >
     > Avoid using the deployment while the temporary CMS runs.
5. Review the confirmation page, and click *Finish*.
   The CCM creates a new node on the destination cluster with the same name and the same servers as the node on the source cluster. A copy of the node remains on the source cluster. The configuration templates for the servers in the node do not move. If any errors occur, review the log file.

   > ⚠ Caution
   >
   > Do not use the source cluster after moving the node.
6. In the CCM, start the moved node.

11.13.6.1.1 Moving a node on Windows using a script

> ⚠ Caution
>
> Back up the server configuration for the entire cluster before and after you move a node.

You can use `MoveNode.bat` to move a node on a Windows machine. For more information, see the “Script parameters for moving nodes” section.

Example

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in these parameters, unless you enclose the text within quotation marks.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
        -username Administrator
```

```
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

> **Note**
>
> To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

Related Information

Variables [page 456]
Script parameters for moving nodes [page 477]

11.13.6.2 To move an existing node on Unix

Context

In this example, the node that you want to move is installed on the source system. The source system machine was initially standalone, but it will be added to the destination cluster.

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you move a node.

Procedure

1. Run `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>` to stop the node.
2. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
3. Select *4 - Move node*, and press `Enter`.
4. Select the node you want to move, and press `Enter`.
5. When prompted, select the system database connection information, and enter the host name, the port, the Administrator credentials for the destination CMS, and the cluster key.
6. Select a CMS.

- If your source deployment is running, select *existing*, and press `Enter`.
  If prompted, enter the host name and port number for the source system's existing CMS and the Administrator credentials.
- If your source deployment is stopped, select *temporary*, and press `Enter`.
  If prompted, enter the host name and port for the source system's temporary CMS, the Administrator credentials, the database connection information and the credentials for the source system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

  > ⚠ Caution
  >
  > Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

7. Review the confirmation page, and press `Enter`.
   The CCM creates a new node on the destination cluster with the same name and the same servers as the node on the source cluster. A copy of the node remains on the source cluster. The configuration templates for the servers in the node do not move. If any errors occur, review the log file.

   > ⚠ Caution
   >
   > Do not use the source cluster after moving the node.

8. Run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the moved node.

11.13.6.2.1 Moving a node on Unix using a script

> ⚠ Caution
>
> Back up the server configuration for the entire cluster before and after you move a node.

You can use `movenode.sh` to move a node on a Unix machine. For more information, see the "Script parameters for moving nodes" section.

Example

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

Related Information

Variables [page 456]
Script parameters for moving nodes [page 477]

11.13.7 Script parameters

11.13.7.1 Script parameters for adding, recreating, and deleting nodes

Parameter	Description	Example
`-adopt`	Recreates the node if it already exists in the CMS.	`-adopt`
`-cms`	The name and port number of the Central Management Server (CMS). **⚠ Caution** Do not use this parameter if you use `-usetempcms` **ⓘ Note** You must specify a port number if the CMS is not running on the default 6400 port.	`-cms mycms:6409`
`-cmsport`	• The port number of the CMS when starting a temporary CMS. **⚠ Restriction** You must also use the `-usetempcms`, `-dbdriver`, `-connect`, and `-dbkey` parameters. • The port number of the CMS when creating a new CMS. **⚠ Restriction** You must also use the `-dbdriver`, `-connect`, and `-dbkey` parameters.	`-cmsport 6401`

Parameter	Description	Example
`-connect`	The connection string of the CMS (or the temporary CMS) system database. **Note** Omit the HOSTNAME and PORT attributes when connecting to DB2, Oracle, SQL Anywhere, SQL Server, or Sybase databases.	`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`
`-dbdriver`	The database driver of the CMS. Accepted values: • `db2databasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlanywheredatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `newdbdatabasesubsystem`	`-dbdriver mysqldatabasesubsystem`
`-dbkey`	The cluster key.	`-dbkey abc1234`
`-name`	The name of a node.	`-name mynode2`
`-noservers`	Creates a node without servers. **Note** The additional `-createcms` parameter creates a node with a CMS, but no other servers. Omit these parameters to create a node with all of the default servers.	`-noservers`
`-password`	The password of the Administrator account.	`-password Password1`
`-siaport`	The port number of the Server Intelligence Agent for the node.	`-siaport 6409`
`-username`	The user name of the Administrator account.	`-username Administrator`
`-usetempcms`	**Caution** Do not use this parameter if you use `-cms` Starts and uses the temporary CMS. **Note** Use a temporary CMS when your deployment is not running.	`-usetempcms`

Related Information

Adding a node on Windows using a script [page 459]
Adding a node on Unix using a script [page 461]
Recreating a node on Windows using a script [page 463]
Recreating a node on Unix using a script [page 465]
Deleting a node on Windows using a script [page 467]
Deleting a node on Unix using a script [page 468]

11.13.7.2 Script parameters for moving nodes

Parameter	Description	Example
`-cms`	The name of the source Central Management Server (CMS). **⚠ Caution** Do not use this parameter if you use `-usetempcms` **ⓘ Note** You must specify a port number if the CMS is not running on the default 6400 port.	`-cms sourceMachine:6409`
`-cmsport`	• The port number of the CMS when starting a temporary CMS. **⚠ Restriction** You must also use the `-usetempcms`, `-dbdriver`, `-connect`, and `-dbkey` parameters. • The port number of the CMS when creating a new CMS. **⚠ Restriction** You must also use the `-dbdriver`, `-connect`, and `-dbkey` parameters.	`-cmsport 6401`

Parameter	Description	Example
`-connect`	The connection string of the source CMS (or the temporary CMS) system database. **Note** Omit the HOSTNAME and PORT attributes when connecting to DB2, Oracle, SQL Anywhere, SQL Server, or Sybase databases.	**`-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`**
`-dbdriver`	The database driver of the source CMS. Accepted values: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	The source cluster key.	**`-dbkey abc1234`**
`-destcms`	The name of the destination CMS. **Note** You must specify a port number if the CMS is not running on the default 6400 port.	**`-destcms destinationMachine:6401`**
`-destconnect`	The connection string of the destination CMS system database. **Note** Omit the HOSTNAME and PORT attributes when connecting to DB2, Oracle, SQL Anywhere, SQL Server, or Sybase databases.	**`-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`**
`-destdbdriver`	The database driver of the destination CMS. Accepted values: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-destdbdriver sybasedatabasesubsystem`**
`-destdbkey`	The destination cluster key.	**`-destdbkey def5678`**

Parameter	Description	Example
`-destpassword`	The password of the Administrator account on the destination CMS.	`-destpassword Password2`
`-destusername`	The user name of the Administrator account on the destination CMS.	`-destusername Administrator`
`-password`	The password of the Administrator account on the source CMS.	`-password Password1`
`-username`	The user name of the Administrator account on the source CMS.	`-username Administrator`
`-usetempcms`	**⚠ Caution** Do not use this parameter if you use `-cms` Starts and uses the temporary CMS. **ⓘ Note** Use a temporary CMS when your deployment is not running.	`-usetempcms`

Related Information

Moving a node on Windows using a script [page 472]
Moving a node on Unix using a script [page 474]

11.13.8 Adding Windows server dependencies

In a Windows environment, each instance of the Server Intelligence Agent (SIA) depends on the Event Log and Remote Procedure Call (RPC) services.

If a SIA does not operate correctly, ensure that both services appear on the SIA's *Dependency* tab.

11.13.8.1 To add Windows server dependencies

Procedure

1. Use the Central Configuration Manager (CCM) to stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and select *Properties*.
3. Click the *Dependency* tab.

4. Click *Add*.
   The *Add Dependency* dialog box appears, displaying a list of all available dependencies.
5. Select a dependency, and click *Add*.
6. Click *OK*.
7. Use the CCM to restart the SIA.

11.13.9 Changing the user credentials for a node

You can use the Central Configuration Manager (CCM) to specify or update the user credentials for the Server Intelligence Agent (SIA) if the operating system password changes, or if you want to run all of the servers on a node under a different user account.

All servers managed by the SIA run under the same account. To run a server using a non-system account, ensure that your account is a member of the Local Administrators group on the server machine, and that it has the "Replace a process level token" right.

> ⚠ Restriction
>
> On a Unix machine, you must run the BI platform with the same account that was used to install it. To use a different account, reinstall the deployment using a different account.

11.13.9.1 To change the user credentials for a node on Windows

Procedure

1. Use the Central Configuration Manager (CCM) to stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and select *Properties*.
3. Clear the *System Account* check box.
4. Enter a username and a password, and click *OK*.
5. Use the CCM to restart the SIA.

Results

The SIA and the server processes log onto the local machine with the new user account.

11.14 Renaming a machine in a BI platform deployment

11.14.1 Changing cluster names

The following are best practices for renaming clusters:

> ⚠ Caution
>
> Never deploy multiple clusters with the same name.

Condition	Action
The name of the cluster changes.	Inform your users of the new cluster name and ask them to use it (after the first connection to the CMS using the `<hostname>:<port>` syntax). On the web tier, update the cluster name in the properties files of all web application servers.
You install a different version of the BI platform on a machine that previously ran a CMS, or you add the machine to a different cluster.	• Ensure that the new CMS runs on a different port. • Use different passwords for different clusters to prevent users from logging into an incorrect cluster.

11.14.2 Changing IP addresses

To avoid configuration changes that result from changes to the machine's IP address, select *Server Properties* on the *Servers* tab of the CMC, and then ensure that all servers bind to hostnames, or use the *Auto-Assign* option. In addition, follow these best practices:

Condition	Action
You use ODBC with the CMS database or the auditing database.	Ensure that the DSN uses the CMS database server hostname.
You use another database connection type with the CMS database or the auditing database.	Use the CCM to update the database to use the database server hostname.
The CMS database or the auditing database is located on the same host at the CMS.	Use `localhost` for the machine name.
You use the URL for BI platform web applications that users access using web browsers (for example, the CMC).	Use hostnames instead of IP addresses for the default URL. To update the URL for the default viewer, select *Processing Settings* for the selected application. For example, for Open Document, click the *Applications* tab in the CMC, right-click *Open Document*, and select *Processing Settings*.
You use the URL for BI platform clients based on web services (for example, Crystal Reports for Java or LiveOffice).	
You use OpenDocument.	

Alternative guidelines

> **Note**
>
> Follow these guidelines only if you cannot follow the best practices described above.

For machines hosting servers

Condition	Action
The host contains BI platform servers, and the servers must bind to specific IP addresses.	Change the IP addresses on the *Servers* tab of the CMC, but do not restart the servers until everything on the machine has been updated. Then reboot the machine; not the individual BI platform servers.
A database connection must use an IP address.	Change the IP address.
An IP address change is required in a static IP network.	Change the IP address of the BI platform machine. **→ Tip** Log on to the CMC to verify that the BI platform is operational.

> **→ Remember**
>
> Restart the machine after performing an action.

For machines hosting the web application server

Condition	Action
The OpenDocument default viewer URL must use an IP address.	Update the IP address in the *Default Viewer URL* field in the *Processing Settings* section of the *Applications* tab of the CMC.
Your users access BI platform web applications (for example, the CMC) by providing a URL with an IP address in their browsers.	Inform your users of the new IP address.
BI platform clients based on web services (for example, Crystal Reports for Java, or LiveOffice) must use IP addresses.	Configure all clients to use the new IP address.

Related Information

Selecting a new or existing CMS database [page 490]

11.14.3 Renaming machines

You can rename machines in a BI platform deployment at any time by stopping all BI platform servers on the machine and then renaming the machine. The following are best practices for renaming machines:

Condition	Action
You log on for the first time.	Use the CMS machine name (rather than the cluster name).
You have a multi-machine deployment.	Ensure that all CMS servers on all other machines are running during renaming.

11.14.3.1 Server tier

> **Note**
>
> Before you rename the CMS machine, inspect the configuration of all servers located on the machine that you would like to rename on the "Server Management" tab of the CMC. If the *Hostname* property uses the old CMS hostname, update it to the new CMS hostname.

> **→ Remember**
>
> Do not restart the servers until you complete all machine renaming procedures.

Follow these instructions for renaming server tier machines:

Condition	Action
The renamed machine hosts a CMS, and users have previously logged in by providing the name of the old machine.	Inform your users of the CMS machine name and ask them to use it.
The renamed machine hosts a CMS, and the BI platform web application default properties files contain the old CMS hostname in the `cms.default` property.	Update the CMS machine name in the `cms.default` property in all custom property files on all web tier machines. On Tomcat, the property files that you create are located in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` by default. **Note** If no custom property files exist, create new custom property files. Copy the the default property files to a custom folder, and remove all content except for the `cms.default` line from the custom property files.
You use Portal Integration Kits or custom applications.	Configure the Portal Integration Kits or custom applications to use the new CMS hostname.

Condition	Action
Your deployment meets all of the following conditions: • A cluster has multiple nodes. • All CMS servers run only on the machine that has been renamed. • At least one node does not host the CMS. • You rename a machine with at least one node. • The IP address changes during the renaming process.	Use the CCM to perform the "Recreate Node" workflow on all nodes, except for the node that hosts the CMS, and then start all BI platform nodes in the deployment. For more information, see the "Managing Nodes" chapter.

→ Remember

Restart the web application or application server after performing an action.

Related Information

Recreating a node [page 462]

11.14.3.2 Web tier

If you rename the machine that hosts the BI platform web application server, follow these instructions:

Condition	Action
You change the name of the machine that hosts the BI platform web application server, and the URL of the default OpenDocument viewer uses a web application server hostname.	Log onto the CMC and update the default viewer URL in *Applications* > *CMC* > *Processing Settings*.
You change the name of the machine that hosts the BI platform web application server, and your users access BI platform web applications using a URL that includes a web application server hostname.	Ask your users to access BI platform web applications using a URL that includes the new web application server hostname.
You change the name of the machine that hosts the BI platform web application server, and web service-based BI platform clients use web application server hostnames in the URL.	Reconfigure all web-service-based BI platform clients to use the new web application server hostname.

11.14.3.3 Databases

If you rename the machine hosting the CMS system database or the auditing database, follow these best practices:

Condition	Action
You want to avoid updating the IP address.	Use the CMS database or auditing database machine name in the data source name (DSN).
The CMS database or auditing database is located on the same host as the CMS.	Use `localhost` in the DSN to avoid updating it if the host-name changes.

CMS system database

Condition	Action
You rename a machine that hosts the CMS system database, and you use ODBC.	Update the CMS database DSN to the new database server hostname.
You rename a machine that hosts the CMS system database, and you use a non-ODBC connection type.	Use the CCM to update the CMS database to the new data-base server hostname on every node in the cluster.

Auditing database

Condition	Action
You rename a machine that hosts the auditing database, and you use ODBC.	Update the auditing database DSN to use the new database server hostname.
You rename a machine that hosts the auditing database, and you use a non-ODBC connection type.	Update the database server machine name to the new data-base server hostname on the *Auditing* tab of the CMC.

11.14.3.4 File Repository Servers

If you rename the machine that hosts the FRS file store, you must update the *Input File Repository* and *Output File Repository* servers on the "Server Management" page of the CMC, and ensure that the *File Store Directory* and *Temporary Directory* properties use the new file store path, and then restart the servers.

11.15 Using 32-bit and 64-bit third-party libraries with BI platform

BI platform servers are a combination of 32-bit and 64-bit processes. Some servers additionally launch 32-bit and 64-bit child processes. To use the correct version of third-party libraries (32-bit vs 64-bit) with BI platform processes, you must set separate 32-bit and 64-bit environment variables on the machines hosting the BI platform. You must then set an additional environment variable that contains a comma-separated list of those

environment variables that have 32-bit and 64-bit versions. When a process is launched by the BI platform, it will select the appropriate variable depending on whether the process is 32-bit or 64-bit.

- `<FIRST_ENV_VAR>`=The value to be used by 64-bit BI platform processes.
- `<FIRST_ENV_VAR32>`=The value to be used by 32-bit processes.
- `<SECOND_ENV_VAR>`=The value to be used by 64-bit processes.
- `<SECOND_ENV_VAR32>`=The value to be used by 32-bit processes.
- BOE_USE_32BIT_ENV_FOR=`<FIRST_ENV_VAR>`,`<SECOND_ENV_VAR>`

For example, if you've installed the BI platform on an AIX machine, as well as 32-bit and 64-bit Oracle clients, and need to set the LIBPATH variable, set the following variables:

- ORACLE_HOME=`<home directory of the 64-bit version of the Oracle client>`
- ORACLE_HOME32=`<home directory of the 32-bit version>`
- LIBPATH=`<library path of the 64-bit version>`
- LIBPATH32=`<library path of the 32-bit version>`
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **Note**
>
> In Linux and Solaris, do not use BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH to separate the 32-bit and 64-bit paths. Instead, add both 32-bit and 64-bit paths to LD_LIBRARY_PATH.

11.16 Managing server and node placeholders

11.16.1 To view server placeholders

Procedure

In the *Servers* management area of the CMC, right-click a server and select *Placeholders*.
The *Placeholders* dialog displays a list of placeholders for all of the servers on the same cluster as the server that you selected. If you want to change the value for a placeholder, modify the placeholder for the node.

Related Information

Server and node placeholders [page 1102]

11.16.2 To view and edit the placeholders for a node

Procedure

1. In the *Servers* management area of the Central Management Console, right-click the node for which you want to change the placeholders, and select *Placeholders*.
2. If you want to edit any of the settings for the placeholders, make the appropriate changes and click *Save* to continue.

> ⚠ Caution
>
> Placeholders other than intended for editing should not be changed in any means. System Administrator should ensure that only the right person from the Administrator group (who are intended for the Node management) should have the edit rights on the Node. All other users including other members of the administrator group should be restricted to view/manage the Node objects by applying the proper security rights. In case if any of the placeholder values is corrupted accidentally and CMS is not coming up, refer to the following SAP Note 3269127.

> ⓘ Note
>
> Please refer to the following SAP Knowledge Base Article 3278916 to know how to restrict placeholders being modified to avoid possible malicious interference with the BI landscape.

Related Information

Server and node placeholders [page 1102]

12 Managing Central Management Server (CMS) Databases

12.1 Managing CMS system database connections

If the CMS system database is unavailable, for example due to a hardware or software failure or a network problem, the CMS goes into the "Waiting for resources" state. If the BI platform deployment has multiple CMSs, then subsequent requests from other servers are forwarded to any CMSs in the cluster that have an active connection to the system database. While a CMS is in the "Waiting for resources" state, any current requests that do not require database access continue to be processed, but requests that require access to the CMS database will fail.

By default, a CMS in the "Waiting for resources" state periodically attempts to reestablish the number of connections that are specified in the "System Database Connections Requested" property. As soon as at least one database connection is established, the CMS synchronizes all necessary data, goes into the "Running" state, and resumes normal operations.

In some cases, you may want to prevent the CMS from automatically reestablishing a connection to the database. For example, you may want to verify the integrity of the database before database connections are reestablished. To do so, on the *Properties* page of the CMS server, uncheck *Auto Reconnect to System Database*.

Related Information

To change a server's properties [page 442]

12.1.1 To select SQL Anywhere as a CMS database

Context

To use SQL Anywhere as a CMS database, you must perform the following steps:

Procedure

1. Stop all nodes in the system.
2. Run the appropriate application:

- On Unix, run `./cmsdbsetup.sh`.
- On Windows, start the Central Configuration Manager (CCM).

3. Copy your data from the default CMS database, selecting SQL Anywhere as the destination database. For more information, see the related link "Copying data from one CMS system database to another".
4. On multi-node deployments, update the CMS data source on every node (except the node on which you copy the database) to the new SQL Anywhere database. For more information, see the related link "Selecting a new or existing CMS database".
5. Ensure that the deployment is operational (for example, log into the CMC and view a report).

Related Information

Copying data from one CMS system database to another [page 495]
Selecting a new or existing CMS database [page 490]

12.1.2 To select SAP HANA as a CMS database

Context

To use SAP HANA as a CMS database, you must perform the following steps.

Procedure

1. Install the BI platform with the default CMS database.
2. Install the SAP HANA client.
3. Create a connection to SAP HANA.
   - On Unix, check the environment variable `ODBCINI`. If the variable exists and points to an existing `odbc.ini` file, add the following lines to that file:

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>
     [NewDB]
     DRIVER=<HANA CLIENT PATH>/libodbcHDB.so
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     DATABASENAME=<DBNAME>
     DESCRIPTION=<DESCRIPTION>
     ```

     `<New_DB_version>` is the SAP HANA version; for example "NewDB 1.0", `<HANA Server IP address>` is the SAP HANA server IP address, and `<HANA server port #>` is the SAP HANA server port number.

If the `ODBCINI` environment variable does not exist, create an `odbc.ini` file in the `<INSTALLDIR>/sap_bobj/enterprise_xi40/` directory, add the above lines to the file, and set the `ODBCINI` environment variable as follows:

```
ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
```

Ensure the ODBCINI environment variable is set in the profile of the user that starts the BI servers.

- On Windows, create an ODBC connection to SAP HANA.

> **Note**
>
> For ODBC connection changes, be sure to run the 64-bit version of the ODBC Data Source Administrator: *Start* > *Control Panel* > *Administrative Tools* > *Data Sources (ODBC)*.

4. Ensure that connections can be made to the SAP HANA server.
   - On Unix, you can test the connection to the SAP HANA server by running the following command. The variables in the following example refer to the SAP HANA installation:

     ```
     <INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID>
     <NONADMINUSER> <NONADMINPASSWORD>
     ```

   - On Windows, you can use the ODBC Data Source Administrator to test the SAP HANA ODBC connection.
5. On Unix, make sure the `LD_LIBRARY_PATH` or `LIBPATH` environment variables contain the path to the `libodbcHDB.so`. For more inforrmation, see 2792543, 1886746, and 2721890.
6. Install the product following the wizard, and select SAP HANA as the CMS / Audit database.
7. Ensure that the deployment is operational (for example, log into the CMC and view a report).

> **Note**
>
> This procedure doesn't apply if you are moving a database from an existing database to an SAP HANA database. If that's the case, use the copy data source procedure. For more information, see Copying data from one CMS system database to another [page 495].

Related Information

Copying data from one CMS system database to another [page 495]
Selecting a new or existing CMS database [page 490]

12.2 Selecting a new or existing CMS database

You can use the CCM or `cmsdbsetup.sh` to specify a new or existing CMS system database for a node. Generally, there are only a few times when you need to complete these steps:

- If you have changed the password for the current CMS system database, these steps allow you to disconnect from, and then reconnect to, the current database. When prompted, you can provide the CMS with the new password.
- If you want to select and initialize an empty database for the BI platform, these steps allow you to select that new data source.
- If you have restored a CMS system database from backup (using your standard database administration tools and procedures) in a way that renders the original database connection invalid, you will need to reconnect the CMS to the restored database. (This might occur, for instance, if you restored the original CMS database to a newly installed database server.)

> **Note**
>
> If you use IBM DB2 as your CMS database, and upgrade it from a version older than 9.5 Fix Pack 5 to version 9.5 Fix Pack 5 or newer (for the 9.5 line), or if you upgrade from a version older than 9.7 Fix Pack 1 to version 9.7 Fix Pack 1 or newer (for the 9.7 line), then during the next restart of the BI platform node or CMS, the CMS database schema will automatically be updated by the CMS to support HADR-compatible schema.
>
> This may be a lengthy process, during which the BI platform system will not be available for use. Do not interrupt the update process, to avoid corrupting the CMS database. It is highly recommended that you back up your CMS database before performing this operation. Also, do not try to use IBM HADR with an IBM DB2 CMS database of a version older than 9.5 Fix Pack 5 (for the 9.5 line) or 9.7 Fix Pack 1 (for the 9.7 line).

> **Note**
>
> Do not configure a BI platform installation to use a CMS system database belonging to a different cluster, unless you are performing a system copy workflow.
>
> System corruption may occur if the versions and patch levels of the BI platform installations and CMS databases are different, or if installation paths differ, or if installed components differ, etc.
>
> To prevent corruption, do not attempt to migrate BI content from one system to another by pointing the BI platform deployment to a CMS database of another BI platform system, especially one of a different version and patch level.

> **Note**
>
> Business Intelligence platform supports SSL communication between the CMS and databases like CMS database and Audit database. For SSL communication,
>
> - You should use SQL Anywhere, SQL Server, and SAP HANA databases as a CMS or Audit database to communicate securely with CMS.
> - You should enable SSL in respective database servers. Refer the documentation specific to your database.
> - You should create an ODBC connection and pass the DB server certificate through this ODBC connection.
> - You should use the same ODBC connection for connecting to CMS database and Audit database.

12.2.1 To select a new or existing CMS database on Windows

Procedure

1. Use the CCM to stop the Server Intelligence Agent (SIA).
2. Select the SIA and click the *Specify CMS Data Source* button.
3. Select *Update Data Source Settings* and click *OK*.
4. Select a database driver and click *OK*.
5. These steps depend upon the connection type you selected:
   - If you selected ODBC, the Windows "Select Data Source" dialog box appears. Select the ODBC data source that you want to use as the CMS database; then click *OK*. (Click *New* to configure a new DSN.) When prompted, provide your database credentials and click *OK*.
   - If you selected a native driver, you are prompted for your database Server Name, your Login ID, and your Password. Provide this information and then click *OK*.
6. Specify the cluster key.
7. Restart the Server Intelligence Agent.

12.2.2 To select a new or existing CMS database on UNIX

Context

Use the `cmsdbsetup.sh` script. For reference, see the "Unix scripts" topic in the Command Line Administration chapter in the *BI platform Administrator Guide*.

Procedure

1. Run the `cmsdbsetup.sh` script (located by default in `<INSTALLDIR>/sap_bobj/`).
2. Select the update action (option 6).
3. When prompted, provide the database type of the new CMS database.
4. Provide the database information (for example: host name, user name, password, and cluster key).
   A notification message appears when the CMS database has been pointed to the new location.
5. If you are prompted to rebuild the Server Intelligence Agent (SIA), provide the administrator password and the port number you want the CMS to communicate on.

> **Note**
>
> You will be prompted for this information only if you point to an empty CMS database.

Related Information

Unix Scripts [page 1004]

12.3 Recreating the CMS system database

This procedure shows how to recreate (reinitialize) the current CMS system database. By performing this task, you destroy all data that is already present in the database. This procedure is useful, for instance, if you have installed the BI platform in a development environment for designing and testing your own, custom web applications. You can reinitialize the CMS system database in your development environment every time you need to clear the system of all its data.

> ⚠ Caution
>
> By implementing the steps outlined in this workflow, you will delete all data in the CMS database as well as objects such as reports and users. Do not perform these steps on a production deployment.

It is very important that you back up all server configuration settings before reinitializing the CMS system database. When you recreate the database, your server configuration settings will be erased and you must have a backup in order to restore this information.

When you recreate the system database, your existing license keys should be retained in the database. However, if you need to enter license keys again, log on to the CMC with the default Administrator account. Go to the Authorization management area and enter your information on the License Keys tab.

> ⓘ Note
>
> If you reinitialize your CMS system database, all data in your current CMS system database will be destroyed. Consider backing up your current database before beginning. If necessary, contact your database administrator.

Related Information

Backing up server settings [page 506]

12.3.1 To recreate the CMS system database on Windows

Procedure

1. Use the CCM to stop the Server Intelligence Agent (SIA).

> **Note**
>
> For this procedure, you cannot run the CCM on a remote machine; it must be run on a machine with at least one valid node. Also, the CMS binaries must be installed on this machine.

2. Right-click the SIA and choose *Properties*.
3. In the *Properties* dialog box, go to the *Configuration* tab and click *Specify*.
4. In the *CMS Database Setup* dialog box, click *Recreate the current Data Source*.

> **Note**
>
> Servers and objects from the machine where you ran the CCM in step 1 will also be recreated. However, not all objects will be recreated; only the key default objects. For example, sample reports are not recreated.

5. Click *OK* and, when prompted to confirm, click *Yes*.
6. Specify the password for the CMS system database, and click *OK*.

> **Note**
>
> Ensure that you set a new administrator password. By default, the Administrator account will have no password.

   The CCM notifies you when the CMS system database setup is complete.
7. Click *OK*.

   You are returned to the CCM.
8. Restart the Server Intelligence Agent and enable services.

   While it is starting, the Server Intelligence Agent starts the CMS. The CMS writes required system data to the newly emptied data source.
9. If your deployment has more than one machine, you need to re-create the nodes on the other machines.

12.3.2 To recreate the CMS system database on UNIX

Context

Use the `cmsdbsetup.sh` script. For reference, see the “Unix scripts” topic in the Command Line Administration chapter in the *BI platform Administrator Guide*.

Procedure

1. Run `cmsdbsetup.sh` (located in `<INSTALLDIR>/sap_bobj/`, by default).
2. Select the "reinitialize" option (option 5), then confirm your choice.
   The `cmsdbsetup.sh` script begins recreating the CMS system database.

3. Provide the CMS system database password.
4. When the database creation is complete, exit the `cmsdbsetup.sh` script.
5. Provide the database information (for example: host name, user name, and password).
   A notification message appears when the CMS database has been pointed to the new location.
6. If you are prompted to rebuild the Server Intelligence Agent (SIA), provide the administrator password and the port number you want to CMS to communicate on.

   > **Note**
   >
   > You will be prompted for this information only if you point to an empty CMS database.

7. In the `<INSTALLDIR>/sap_bobj/` directory, use the following command to start the node.

   ```
   ccm.sh -start <nodename>
   ```

8. To enable the services, use the following command:

   ```
   ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password
   <password>
   ```

   > **Note**
   >
   > Since you just recreated the CMS database, the administrator password is blank.

Related Information

Unix Scripts [page 1004]

12.4 Copying data from one CMS system database to another

You can use the Central Configuration Manager (CCM) or `cmsdbsetup.sh` to copy system data from one database server into another database server. For example, if you want to replace the database with another database because you are upgrading the database or are moving from one database type to another, you can copy the contents of the existing database into the new database before decommissioning the existing database.

The destination database is initialized before the new data is copied in, so any existing contents of the destination database are permanently deleted (all BI platform tables are destroyed permanently and then recreated). Once the data has been copied, the destination database is established as the current database for the CMS.

> **Caution**
>
> Never attempt to use a CMS database from another BI platform cluster. Before starting this workflow, always ensure that the source CMS database was used with this BI platform cluster, and not with another BI platform cluster.

> ⚠ Caution
>
> Never attempt to perform an upgrade by using the CMS database copy workflow. The CMS database copy workflow is designed for moving a CMS database from one database server to another database server. It is not designed for upgrading the CMS database. Before starting this workflow, always ensure that the source CMS database was used with this BI platform cluster, and that it has the same version and patch levels as the current BI platform installation.

12.4.1 Preparing to copy a CMS system database

Before copying a CMS system database, take the source and the destination environments offline by disabling and subsequently stopping all servers. Back up both CMS databases, and back up the root directories used by all Input and Output File Repository Servers. If necessary, contact your database or network administrator.

Ensure that you have a database user account that has permission to read all data in the source database, and a database user account that has Create, Delete, and Update rights to the destination database. Also ensure also that you can connect to both databases—through your database client software or through ODBC, according to your configuration—from the CMS machine whose database you are replacing.

If you are copying a CMS database from its current location to a different database server, your current CMS database is the source environment. Its contents are copied to the destination database, which is then established as the active database for the current CMS. This is the procedure to follow if you want to move the default CMS database from the existing default database to a dedicated database server, such as Microsoft SQL Server, Informix, Oracle, DB2, or Sybase. Log on with an administrative account to the machine that is running the CMS whose database you want to move.

> ⓘ Note
>
> When you copy data from one database to another, the destination database is initialized before the new data is copied in. That is, if your destination database does not contain the BI platform system tables, these tables are created. If the destination database does contain the BI platform system tables, the tables will be permanently deleted, new system tables will be created, and data from the source database will be copied into the new tables. Other tables in the database are unaffected.

> ⓘ Note
>
> If you are copying a CMS system database to a MaxDB destination database on Windows, you must ensure that the path to the MaxDB client has been added to the `<PATH>` environment variable. For example, `;C:\Program Files\sdb\MAXDB1\pgm`.

12.4.2 To copy a CMS system database on Windows

Prerequisites

Before you copy the contents of the CMS database, ensure that you can logon to the destination database with an account that has permissions to add or drop tables, and to add, drop, or modify data in those tables.

Procedure

1. Open the Central Configuration Manager (CCM) and stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and choose *Properties*.
3. Click the *Configuration* tab, and then click *Specify*.
4. Choose *Copy*, then click *OK*.
5. Select the database type for the source CMS database, and then specify its database information (including host name, user name, and password).
6. Select the database type for the destination CMS database, and then specify its database information (including host name, user name, and password).
7. When the CMS database has finished copying, click *OK*.

12.4.3 To copy data from a CMS system database on UNIX

Context

Before you copy the contents of the CMS database, ensure that you can logon to the destination database with an account that has permissions to add or drop tables, and to add, drop, or modify data in those tables.

> **Note**
>
> On UNIX you can not migrate directly from a source environment that uses an ODBC connection to the CMS database. If your source CMS database uses ODBC, you must first upgrade that system to a supported native driver.

Procedure

1. Stop the CMS by typing the following command:
   ```
   ./ccm.sh -stop <nodename>
   ```
2. Run `cmsdbsetup.sh` (located in `<INSTALLDIR>/sap_bobj/`, by default).
3. Select the "copy" option (option 4), then confirm your choice.
4. Select the database type for the source CMS database, then specify its database information (including host name, user name, and password).
5. Select the database type for the destination CMS database, and then specify its database information (including host name, user name, and password).
   The CMS database is copied to the destination database. A message appears when the copy is complete.

12.5 Central Management Server Database Driver

You can now access the CMS Repository Database of BI platform for reporting analysis leveraging existing platform features (Connection Server, Semantic Layer, Reporting clients). SAP BusinessObjects Data Access Driver enables you to use a universe to query the CMS Database. For more information, refer http://scn.sap.com/docs/DOC-74580 .

13 Backing Up and Restoring Your System

13.1 Overview of backup and restore

This chapter explains how to back up the BI platform and how to recover your system from hardware failure, software failure, and data loss. To execute a backup and recovery plan, you need an experienced SAP BusinessObjects Professional, System Administrator, and Database Administrator.

Related Information

Backing up the entire system [page 502]
Backing up BI content [page 509]
To back up server settings in the CCM on Windows [page 506]
To back up server settings on Unix [page 507]
Overview of system copying [page 524]

13.2 Terminology

Term	Definition
Data replication	Data replication is the process of creating one or more copies of your data. The copies are updated in real time; for example, when using mirrored drives. It offers real time data protection from physical data damage, but because the drives are constantly being updated it is not possible to revert your system to an earlier state if data becomes corrupted or accidentally removed.
Versioning	Versioning creates multiple versions of a specific file or files on your system. In this case, it is possible to revert your system to an earlier state. All data versions are typically stored on the same host system. If this system is compromised or damaged, you risk losing both the current version and the older versions. Similarly, Undelete functions keep copies of "deleted" files for later recovery, but again these are usually stored on the same host system as the original data. It doesn't offer protection from physical data damage (for example, disc failure).

Term	Definition
Bare-metal system backup	A bare-metal system backup is a backup of an entire file system, including the operating system. A bare-metal system backup is intended to be used to restore a backed-up system to hardware that contains no software or operating system. For bare-metal system backups, in case of failure, the entire file system (including the OS) is restored to identical hardware, or, if your restore tools support hardware-independent restore, to any hardware.
Bare-metal system backup vs. application backup	A bare-metal system backup creates a copy of the entire system, including the operating system. A bare-metal system backup allows you to revert to an earlier version of the system as a whole. An application backup backs up files related to individual applications. The BI platform supports bare-metal system backups but not application backups. For bare-metal system backups, in case of failure, the entire file system (including the OS) is restored to identical hardware, or, if your restore tools support hardware-independent restore, to any hardware. A complete BI platform system backup is called a backup set.
Backup set	A backup set comprises these individual backups, created at the same time: • A backup of the CMS system database • A bare-metal backup of the entire file system, including the operating system, of all machines in the BI platform deployment • A backup of the Input FRS and the Output FRS file stores (if not included in the BI platform file system) • A backup of the web tier components (if not included as part of the BI platform file system) • A backup of the auditing database
Cold vs. hot backup	A cold backup is performed while the system is stopped and unavailable to users. A hot backup is performed while the system is running and available to users, and data can change while the backup is being performed. Also, when performing a hot backup, you must perform the backup steps in order, which is not the case with a cold backup. The BI platform supports both cold and hot backups. Hot backup is sometimes called “online backup”.

13.3 Use cases for backup and restore

The following table describes the goals you might want to achieve given the resources you might have, and directs you to the most appropriate backup solution.

Goal	Resources required	Solution
Goal: Restore a system 1. My BI platform system was corrupted. Therefore, I need to restore it to the working state it was in when it was last backed up. 2. A machine hosting the BI platform was damaged. I need to replace it with a new machine.	• A target system with identical hardware to the source system AND • Backups of the source system	Use the system backup and restore workflow detailed in this guide. See the Backing up the entire system [page 502] procedure. Recreate the target system from backups of the source system.
Goal: Restore objects I want to recover a document or other object that was accidentally deleted.	• Backups of the source system databases and files AND • Detailed system information described in To export from a source system [page 528]	Using backups, build a copy of the system on another machine, using the System Copy workflow in the "Copying your BI platform deployment" chapter. Then, use the promotion management tools to promote the accidentally deleted objects from that new system. See the System Copy workflow, starting with Planning to copy your system [page 525], and follow the instructions for the rest of the chapter. **Note** You can create your target system on a computer with an existing BI platform deployment of the same release, support package, and patch level, or a "clean" computer with no BI platform installed.
Goal: Restore objects 2 I want to recover a document or other object that was accidentally deleted.	A system where promotion management versioning is in use	Use the promotion management application to recover an earlier version of the document. For details, see the related topic on promotion management.

Note

Backing up the system before and after a software upgrade:

CMS is associated with the 'version' of a product. You cannot use SAP BusinessObjectsBusiness Intelligence platform system, with CMS and FRS from a different version. You must always backup both the CMS and the FRS file store, before and after any software upgrade. If you 'restore' to rollback a software upgrade, you need to ensure the CMS, the FRS, and the software, all belong to the same version.

Related Information

Backups [page 502]
Planning to copy your system [page 525]
Overview [page 535]

13.4 Backups

A backup and recovery plan consists of steps to take in the event of a system failure due to a natural disaster or unexpected failure. The plan aims to minimize the effects of the disaster on daily operations so that you can maintain or quickly resume critical functions.

When backing up your BI platform deployment, you have three options:

- Backing up the entire system, which allows you to restore the entire system. In this case, restoring only a portion of the system is not possible. If you want to rebuild the BI platform instead of restoring it from a backup, see the related topic describing system copying.
- Backing up server settings, which allows you to restore only server settings without restoring other objects, preserving the current state of your system's BI content.
- Backing up BI content (for example, documents), which allows you to selectively restore parts of BI content without the need to restore all objects.

See the related topics for details on all three types of backups.

> → Tip
>
> To avoid data loss, regularly perform backups.

> → Tip
>
> You can back up a BI platform system and then restore it to the same or a different host computer to create a copy of the system.

Related Information

Backing up the entire system [page 502]
Backing up server settings [page 506]
Backing up BI content [page 509]
Overview of system copying [page 524]

13.4.1 Backing up the entire system

Back up your entire BI platform system by performing a cold or hot backup, which creates a backup set. Keeping multiple backup sets from different times gives you more options when restoring the system. Back up your system as frequently as your organization's business needs require.

You can choose to stop your BI platform system and perform a cold backup, or you can perform a hot backup. With a hot backup, the system stays live and available to users during the backup process. It has the advantage of no downtime for your system.

> **Note**
>
> We recommend writing the transaction log to a file system other than the main database server system, regularly backing up this transaction log, and keeping it with the other files in the backup set.

> **Note**
>
> If you back up auditing data, make sure to include the database transaction log for the auditing database with your backup file set. You do not need to include the auditing temporary files with the backup.

13.4.1.1 Hot backups

The hot backup feature allows you to back up your BI platform system while continuing to allow users to use the system normally. If your business must continue operating while your system is backing up, enable and configure hot backups in the Central Management Console.

The *Hot Backup Maximum Duration* setting specifies the maximum amount of time that you expect the backup to take—from the time when the CMS backup begins to the time when the FRS backup ends. If the duration you specify is too short, files may be deleted before the backup has a chance to copy them. To avoid this, it is safer to overestimate the time required. Balance this concern against system resources because a high value may slightly increase your FRS file store size.

> **Note**
>
> - Hot back up does not actually perform a backup, it just delays the deletion of files. When files are edited or updated, multiple copies are held. This means the CMS and the FRS always maintain the correct relationships, allowing for a backup of each to be taken at different times. However, this happens within the hot backup window.
> - When you restore the system, you end up with many extra files in the FRS that the Repository Diagnostic Tool needs to delete.
> - Always initiate the CMS backup prior to backing up the FRS file store.
>
> Hot backup is enabled as long as the *Enable Hot Backup* check box is selected in the CMC; the *Hot Backup Maximum Duration* setting does not affect whether or not hot backup is enabled.

It is easiest to restore your system to a specific backup time. For example, if your system backups are performed daily at 3:00 AM, you can easily restore the system to the state it was in when the CMS system backup started (3:00 AM on the date of your choice). After a CMS database or auditing database failure, if you have enabled transaction logging on the CMS database or the auditing database, you can restore the system to the state it was in immediately before the failure.

For maximum safety, save transaction logging records at a different location than your primary database backup records. This ensures that, in the case of database failure, you can restore the database to the state it was in prior to failure.

> **Note**
>
> Due to a limitation on transaction log size on older versions of IBM DB2, hot backup and transaction-log-related tasks are supported only if the CMS system database is hosted on DB2 database server version 9.5 Fix Pack 5 or newer (for the 9.5 line), and 9.7 Fix Pack 1 or newer (for the 9.7 line).

> **Note**
>
> We recommend writing the transaction log to a file system other than the main database server system, regularly backing up this transaction log, and keeping it with other files in the backup set.

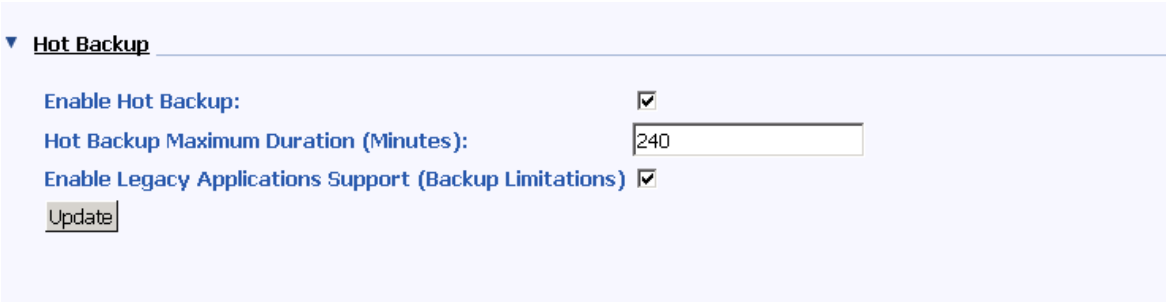
13.4.1.1.1 To enable hot backups

Procedure

1. Open the Central Management Console (CMC).
2. From the *Manage* area, open the *Settings* page.
3. In the *Hot Backup* section, select *Enable Hot Backup*.
4. Enter the maximum number of minutes you expect the backup to take under *Hot Backup Maximum Duration (Minutes)*.

   Be sure to include the time required to back up both the CMS database and the file system of the BI platform host machine.

   > **Note**
   >
   > If the actual duration of the backup exceeds the limit entered here, it may cause inconsistencies in the backed-up data. To avoid this, it is safer to overestimate the time required.
5. Click *Update*.
   Hot backup is enabled.



Next Steps

Once hot backup support is enabled, you can perform backups using your database and file system vendor's backup tools.

13.4.1.2 To perform a hot or cold system backup

Prerequisites

If you want to perform a hot backup, first see the related topic about hot backups for prerequisites and more information. If you are performing a cold backup, stop all nodes in your BI platform deployment.

> ⚠ Caution
>
> If you perform a backup without enabling hot backup and without stopping all nodes, data inconsistencies may result between the CMS database and the FRS file store.

Context

> ⓘ Note
>
> For hot backups, it is important that the procedures are started in the sequence described. For cold backups, the procedures can be performed in any order. In either case, it is not necessary to wait for each backup step to complete before starting the next step.

Procedure

1. Use your database vendor tools to back up the Central Management Server (CMS) system database.

   > ⓘ Note
   >
   > For hot backups, use the database vendor's backup tools in online atomic mode.

2. Use your database vendor tools in online atomic mode to back up the BI platform auditing database.
3. Back up the entire file system, including the operating system, of all machines in the BI platform deployment. For Unix machines, backup the install directory and the home directory of install account.
   a. If the Input and Output FRS file stores are not included in the BI platform backup (separate host machines), create a backup copy of both using your file-backup tools.
   b. If the web-tier components are not included in the BI platform backup (separate host machines), create a backup copy of them using your file backup tools.

   For hot backups, use atomic file backup tools if possible.

Next Steps

If you performed a cold backup, wait for all backups to complete and then start your BI platform nodes.

Related Information

Hot backups [page 503]

13.4.2 Backing up server settings

In order to protect your system from misconfigured server settings, back up your server settings to a BIAR file on a regular basis. Having available backups of your servers allows you to restore settings without having to restore your Central Management Server (CMS) system database, File Repositories, or Business Intelligence content.

It is essential that you back up your server settings whenever you make any changes to your system's deployment. This includes creating, renaming, moving, and deleting nodes, and creating or deleting servers. It is recommended that you back up your server settings before you change any of the settings, and then again after you're satisfied with the changes that you've made.

> **Note**
>
> Backing up the server settings is not an additional task to the backup of CMS and FRS file store, i.e. a restore of the CMS/FRS also restores the server settings. Server settings backup is a small subset of a complete backup of the CMS database. You do not need to restore the server settings if you have already restored the CMS.

Use the Central Configuration Manager (CCM) or a script to back up your BI platform server settings to a BIAR file, and then store the file on a separate machine or storage media.

> **Note**
>
> If you are backing up or restoring server settings in a deployment where SSL is enabled, you must first disable SSL through the CCM, and then re-enable it when the backup or restore is complete.

On Windows, the `BackupCluster.bat` script is located in the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` directory.

On Unix, the `backupcluster.sh` script is located in the `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts` directory.

13.4.2.1 To back up server settings in the CCM on Windows

Context

This procedure backs up the server settings for an entire cluster. It is not possible to back up the settings for individual servers.

> **Note**
>
> If you are using a temporary CMS, you must use the CCM on a machine that has a local CMS binaries installed.

Procedure

1. Start the CCM, and on the toolbar, click *Back up Server Configuration*.
   The *Server Configuration Backup Wizard* appears.
2. Click *Next* to start the wizard.
3. Specify whether to use an existing CMS to back up server configuration settings or to create a temporary CMS.
   - To back up server settings from a system that is running, select *Use existing running CMS*, and click *Next*.
   - To back up server settings from a system that is not running, select *Start a new temporary CMS*, and click *Next*.
4. If you are using a temporary CMS, select a port number for the CMS to run on, and specify the database connection information.

   To minimize the risk of users accessing your system while you are restoring your system, specify a port number that is different than the port numbers that your existing CMS uses.
5. Enter the cluster key, and click *Next* to continue.
6. When prompted, log on to the CMS by specifying the system and user name and password of an account with administrative privileges, and click *Next* to continue.
7. Specify the location and name of a BIAR file that you want to back up the server configuration settings to, and click *Next* to continue.
   The *Confirmation* page displays the information that you have provided.
8. Verify that the information displayed on the *Confirmation* page is correct, and click *Finish* to continue.
   The CCM backs up the server configuration settings for the entire cluster to the BIAR file that you specify. Details of the backup procedure are written to a log file. The name and path of the log file are displayed in a dialog box.
9. If the backup operation failed, check the log file to determine the reason.
10. Click *OK* to close the wizard.

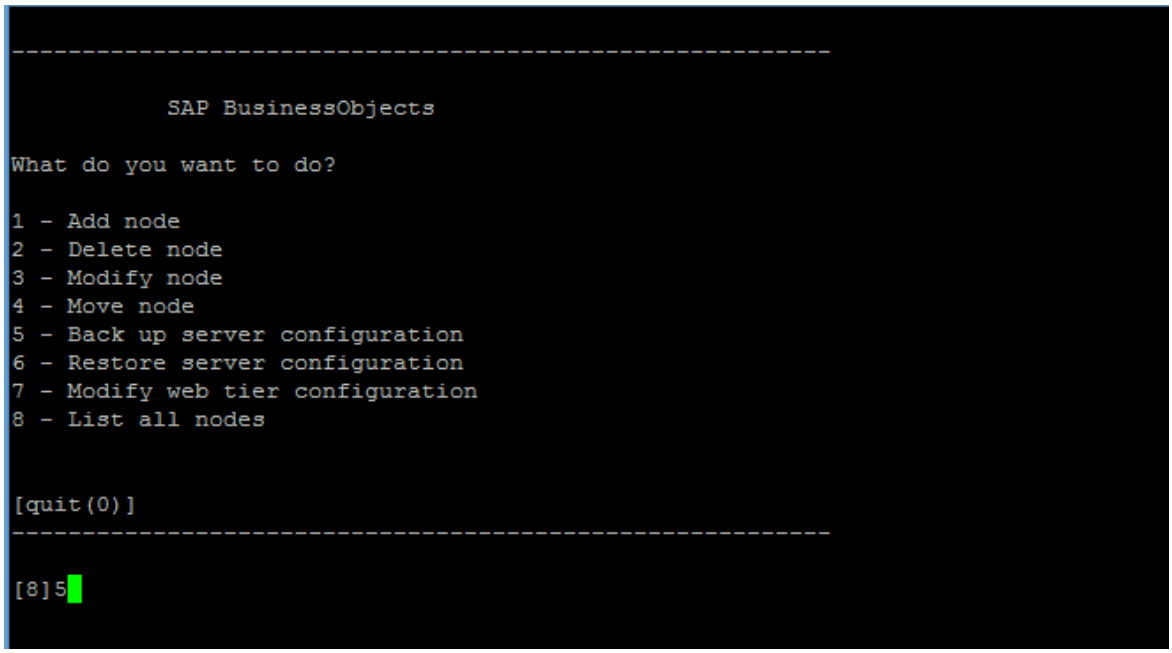
13.4.2.2 To back up server settings on Unix

Context

On Unix, use the `serverconfig.sh` script to back up your deployment's server settings to a BIAR file.

Procedure

1. Select *5 - Back up server configuration* and press `Enter`.



2. Specify whether to use an existing CMS to back up server configuration settings or to create a temporary CMS.
   - To back up server settings from a system that is running, select *existing*, and press `Enter`.
   - To either back up server settings from a system that isn't running, or to restore server settings, select *temporary*, and press `Enter`.
3. If you are using a temporary CMS to back up your server settings, on the next several screens, select a port number for the temporary CMS to run on, and the connection information to the CMS system database.

   To minimize the risk of users accessing your system while you are restoring your system, specify a port number that is different than the port numbers that your existing CMS uses.
4. When prompted, log on to the CMS by specifying the system and user name and password of an account with administrative privileges, and press `Enter`.
5. When prompted, specify the location and name of a BIAR file that you want to back up the server configuration settings to, and press `Enter`.
   A summary page displays the information that you have provided.
6. Verify that the information displayed is correct, and press `Enter` to continue.
   The `serverconfig.sh` script backs up the server configuration settings for the entire cluster to the BIAR file that you specify. Details of the backup procedure are written to a log file. The name and path of the log file are displayed.
7. If the backup operation failed, check the log file to determine the reason.

13.4.2.3 To back up server settings with a script

Context

You can back up the server settings in your deployment by running the `BackupCluster.bat` file on Windows or the `backupcluster.sh` script on Unix.

On Windows, the `BackupCluster.bat` file is located in the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` directory.

On Unix, `backupcluster.sh` is located in the `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts` directory.

Related Information

BackupCluster and RestoreCluster scripts [page 521]

13.4.3 Backing up BI content

It is recommended that you use standard Database and File backup tools and procedures to regularly back up:

- The CMS Database.
- The Input FRS and the Output FRS File stores.

Having current backups of your content makes it possible to restore your Business Intelligence without having to restore your entire system or your server settings.

For more information about backing up your system, see To perform a hot or cold system backup [page 505]

13.5 Restoring your system

If your system is damaged or corrupted, you can restore the entire system, which restores the BI platform. Depending on the condition of your system, a complete restoration may not be required. If the system is working normally but you have lost or corrupted content, you can choose to restore only Business Intelligence (BI) content. If BI content is valid but your platform servers have become misconfigured, you can restore only server settings.

The procedure is the same for restoring from a hot or cold backup.

Related Information

Restoring your entire system [page 510]
Restoring server settings [page 517]
Restoring BI content [page 521]

13.5.1 Restoring your entire system

When you restore the entire system, the BI platform cluster is also restored. Depending on what failed in the system, you may still have the option to do only a partial restore.

If any of the following components fails or is lost, you must restore your entire system:

- The CMS database

  > **Note**
  >
  > If the database service crashes, you can just restart the service, without restoring the entire system.

- The FRS file store
- The machine's file system

> **Note**
>
> For a full system restore, the target system does not require the BI platform to be already installed.

If only the auditing database is corrupted or lost, you can restore the auditing database, without restoring the entire system.

If your web-tier content is corrupted or lost, you can restore the web-tier content, without restoring the entire system.

Related Information

To restore your entire system [page 511]
To restore only the auditing database [page 513]
To restore web-tier content [page 513]
To restore only the CMS database [page 514]

13.5.1.1 To restore your entire system

Prerequisites

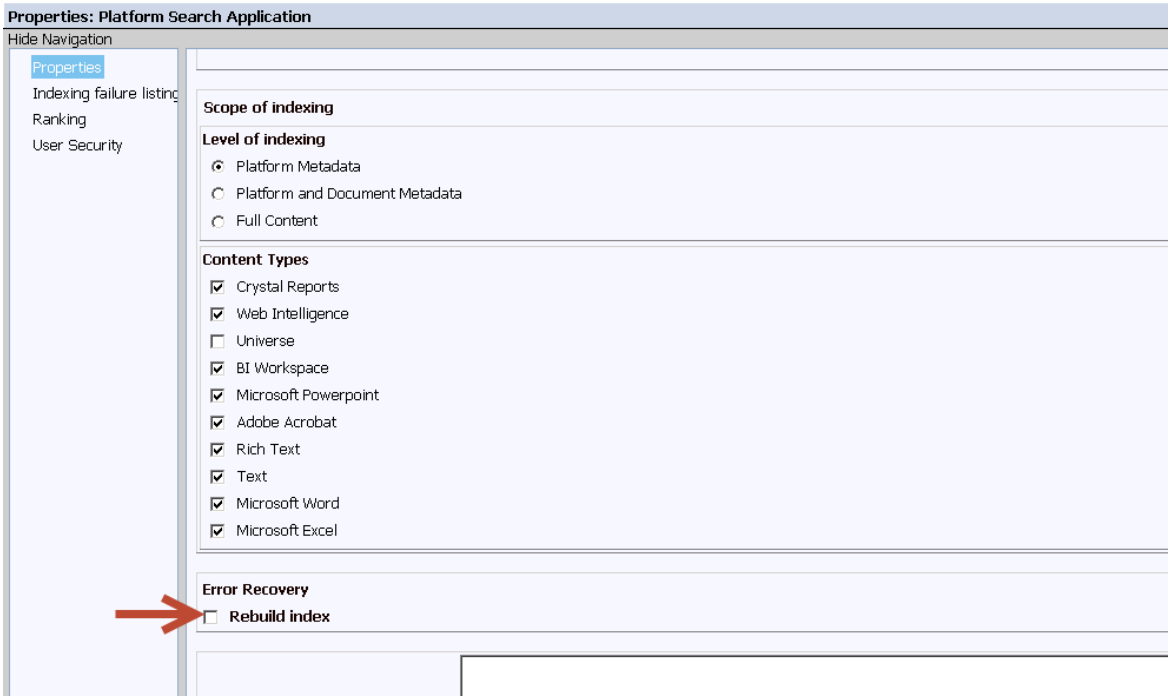
Before restoring your system, you must use the Central Configuration Manager (CCM) to stop all nodes in your BI platform deployment, and you must choose the point in time when you want to restore the system to.

> **Note**
>
> If you may want to restore the system to its current state, back up the system before restoring it.

Procedure

1. Locate the following backup files:
   - CMS database backup
   - Input FRS and Output FRS file store backups
   - Backups of file systems for every host machine in the BI platform cluster

   > **Note**
   >
   > - Make sure to validate the backups, and ensure that all of the files listed above are from the same backup set.
   > - When performing backup and restore, the CMS and the FRS are treated as a single unit. If you restore one of them, you need to restore the other at the same time.
   > - If the backup set was obtained as a hot backup, ensure that the CMS database backup start timestamp is earlier than the matching FRS file store, web tier, and host-machine file-system timestamp. All these files will be required, even if only one component failed.
2. Use your file restore tools to restore the file system of all host machines in the BI platform cluster.
3. Use your file restore tools to restore the Input and Output FRS file stores.
4. Use your database tools to restore the CMS database.
5. If you have changed the CMS database password since the backup was created, use the CCM to update the CMS database password on all nodes and BI platform host machines.
6. If you use the Auditing feature, use your database tools to restore Auditing database.
7. Choose one of the following options for restoring your search index:
   - If you want to run the search index recovery script, see To run the search index recovery script [page 516] and follow the instructions there. This will provide you with a full index more quickly.
   - If you want to rebuild your search index rather than use the recovery script, use the CCM to restart your BI platform nodes. This is a simpler procedure, but while the index is rebuilding you will have only partial search access to the platform data.



8. Start the system, and note the time for use during the post-requisite steps.
9. Verify that your system is working as expected, and perform a sanity test.

Next Steps

Once the system has been verified, take the following actions:

- Run the Repository Diagnostic Tool to remove any unused temporary files and check repository consistency. See the Repository Diagnostic Tool section of this guide.
- If you did not use the index recovery script, rebuild your platform search index.
- Any publishing jobs in process at the time the system was backed up will display as failed. Do not rerun these instances; start new publishing jobs.
- If your auditing database was restored, then you must run an SQL query to remove any events that fall between the database failure and the restart time (the time you noted in step 8). For example: `delete from [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

Related Information

Indexing Content in the CMS Repository [page 871]

13.5.1.2 To restore only the auditing database

Before restoring your auditing database, use the Central Configuration Manager (CCM) to stop all nodes in your BI platform deployment. You must also choose which point in time you want to restore the database to.

> **Note**
>
> Perform this task only if you are sure the auditing database is the only compromised component of the BI platform. If additional components are affected, you must perform a full system restore.

Use your database tools to restore Auditing database.

Related Information

To restore your entire system [page 511]

13.5.1.3 To restore web-tier content

Prerequisites

Before you restore your web-tier content, you must stop all nodes in your BI platform deployment using the Central Configuration Manager (CCM). You will also need to decide which point in time you want to restore the web-tier content to.

If you want to have the option to return to the current state of the system, you must perform a backup of the system before restoring.

Context

If the web-tier is corrupted it can be restored individually.

Procedure

1. Use file restoration tools to restore the web tier folders on the web-tier host-machine.
2. Use the CCM to restart all nodes for your BI platform deployment.

13.5.1.4 To restore only the CMS database

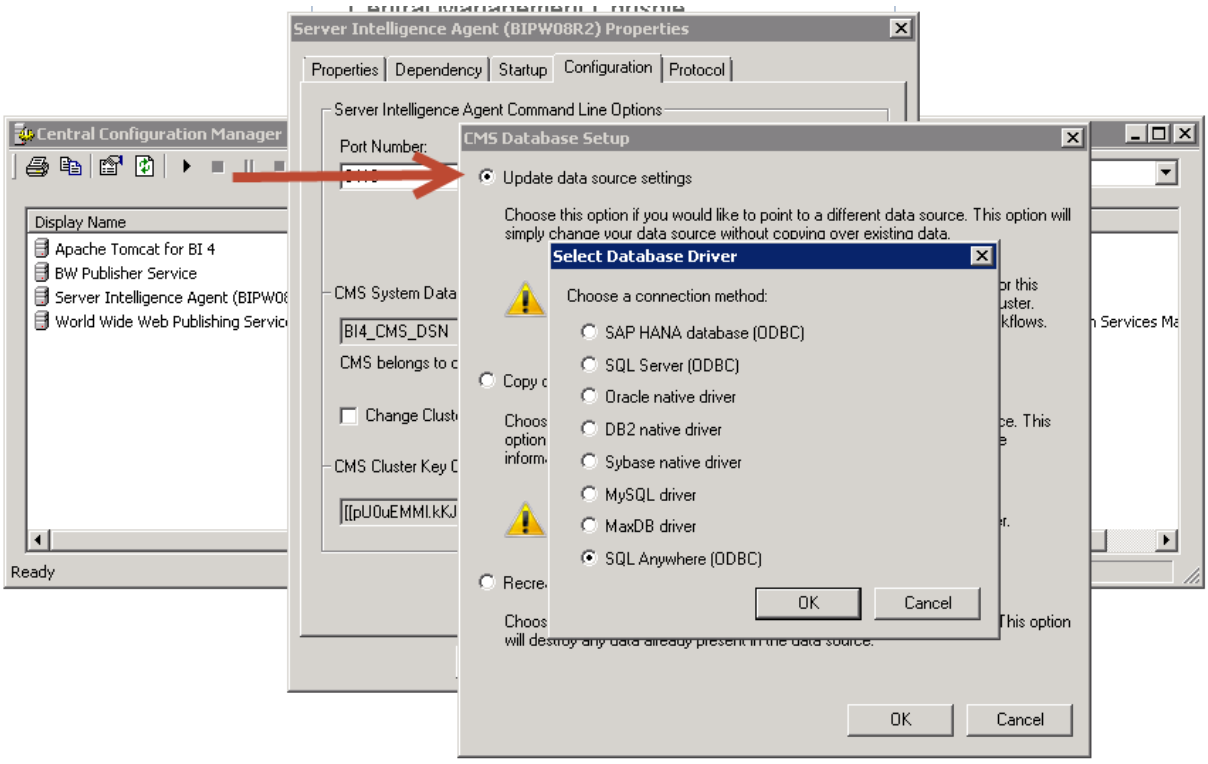
Prerequisites

> **Note**
>
> If the database service crashes, you can just restart the service, without restoring the entire system. If the database is corrupted or other components have been compromised you must perform a full system restore.

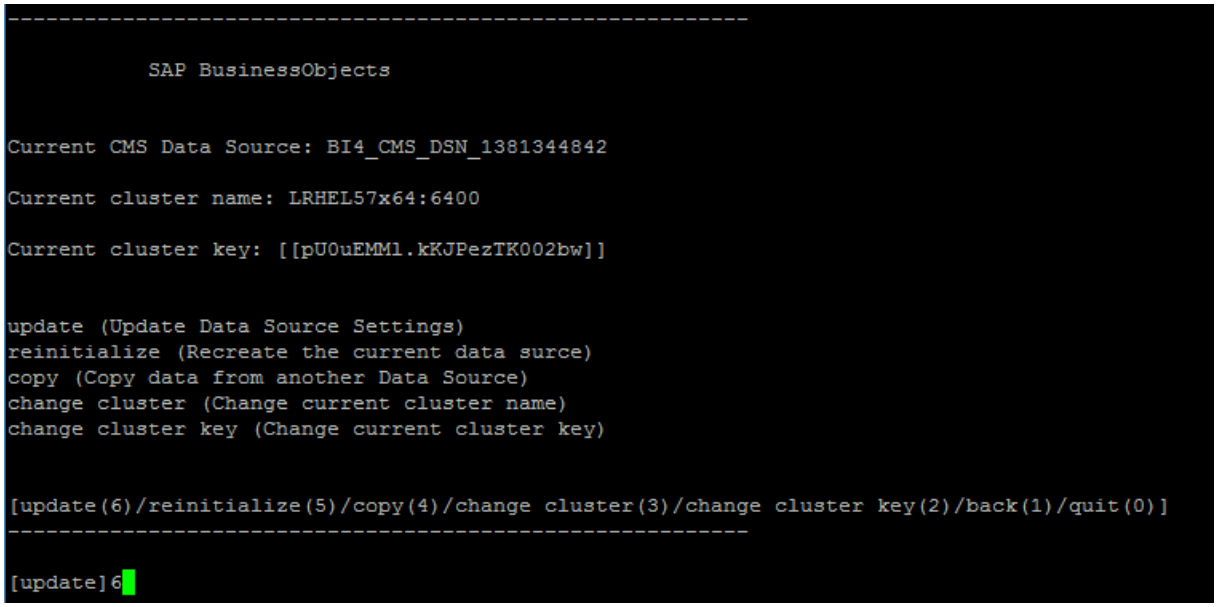
Repair or replace the CMS database host-machine. If replaced, ensure that it has the same system name as the previous host-machine, as well as the same port settings and database credentials.

> **Note**
>
> If it is not possible to restore the machine using the same name and credentials, you will need to use the CCM to update this database connection information for each node in the cluster and restart those nodes.

For Widows:



For Unix: Execute cmsdbsetup.sh, enter node name when prompted, then choose option 6 `update`.



Procedure

1. Stop all BI platform nodes using the CCM.
2. Use your database tools to restore Auditing database.
3. Use the CCM to start the BI platform nodes.

Next Steps

Once you have verified the system is working properly, take the following actions:

- Run the Repository Diagnostic Tool to remove any unused temporary files and check repository consistency. See the Repository Diagnostic Tool section of this guide.
- Any publishing jobs in process at the time the system was backed up will display as failed. Do not rerun these instances; start new publishing jobs.

Related Information

Indexing Content in the CMS Repository [page 871]

13.5.1.5 The search index recovery

The platform search feature maintains a series of index and information files across your system to help it search more efficiently. If it is necessary to restore the system, these information files may develop

inconsistencies. You can repair these inconsistencies by either using the index recovery script or rebuilding the index.

Rebuilding the index is a straightforward procedure, but the process will consume significant resources and take some time to complete, and searches conducted during the rebuild will only return results for the indexed portions of the database. The recovery script involves a more complicated procedure, but will provide you with a full, working index more quickly.

If you are restoring a deployment with multiple computers, run the script on any computers hosting the search service. For the first computer in a cluster, use the `-Both` option, then on all subsequent computers in that cluster, use the `-ContentStore` option.

Related Information

Indexing Content in the CMS Repository [page 871]

13.5.1.5.1 To run the search index recovery script

Prerequisites

- Confirm that the CMS is running, and stop all Adaptive Processing Servers (APS) with the Search Service installed.

  > ⓘ Note
  >
  > You must stop these APSs as quickly as you can after the node starts.

- Set `JAVA_HOME` to the `sapjvm/bin` location in the BI platform installation directory.
- The Platform Search data directory is accessible from the machine where you are running the script.

Procedure

1. On the CMS or APS host-machine, open a command-line window (if using a Windows OS).
2. Switch to the following directory `<INSTALLDIR>\SAP BuinsessObjects Enterprise XI 4.0\java\lib\`.

   Unix machines use the equivalent Unix file path.
3. Type `java -jar platformSearchOnlineHotbackupRestore.jar` and press *Enter*.
4. When prompted, enter the following information and press *Enter*:
   - Your BI platform installation location (for example, `<INSTALLDIR>/SAP businessObjects Enterprise XI 4.0`)
   - Your CMS logon credentials, including the CMS name, user ID and password, and authentication type. Authentication type has the following options:

- `secEnterprise`
- `secLDAP`
- `secWinAD`
- `secSAPR3`

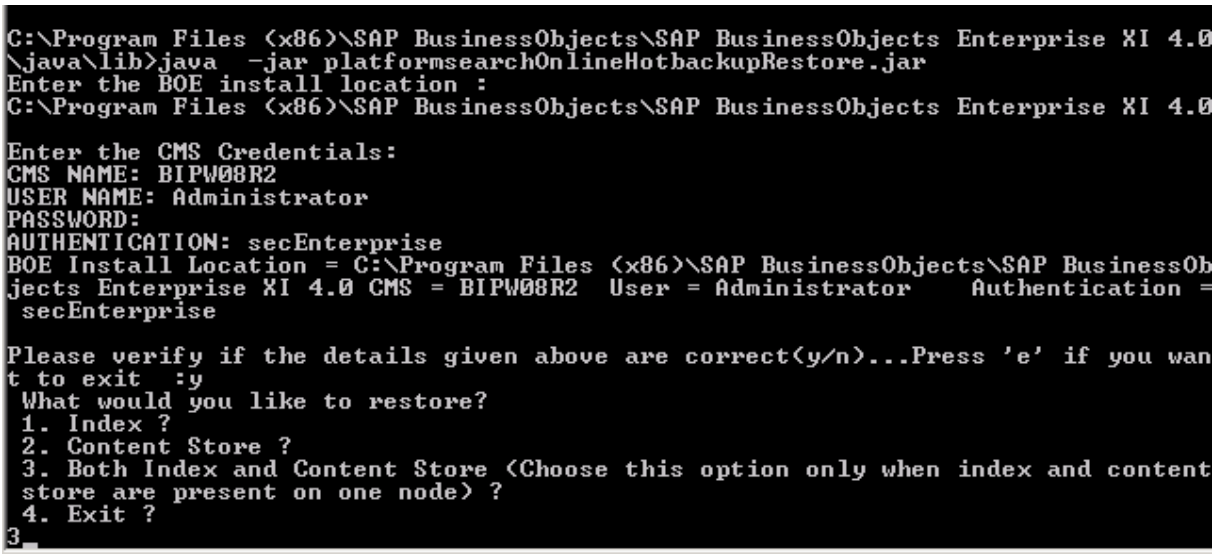
5. When you are prompted for the index restore type, type one of the following options and press *Enter*.

Value	Description
`-Both`	This should be used for single server deployments, or, in multi-machine deployments, for the first APS host-machine with the search service: On a system with multiple search APSs, the first time the script is run, use the `-Both` value (updates the database and content store). When the script is run for all other search APSs, use the `-ContentStore` value (updates only the content store).
`-ContentStore`	This should be used when running the script on APS host-machines with the search service installed, unless it is the first computer in the cluster where the script is run.
`-Exit`	Exit the script without performing an index restore.

6. When the script has finished running, close the command-line window (for Windows machines).

Next Steps

Start all stopped APSs.



13.5.2 Restoring server settings

If you need to restore your system's server settings from a BIAR file, you can use either the Central Configuration Manager (CCM) or the RestoreCluster script to restore the server settings. Restoring server

content from a BIAR file doesn't affect Business Intelligence content such as reports, users and groups, or security settings.

> **Note**
>
> When restoring server settings, only the restoration of the settings for an entire cluster is supported. It is not possible to restore the settings for only some of the servers in the cluster.

> **Note**
>
> If you are backing up or restoring server settings in a deployment where SSL is enabled, you must first disable SSL through the CCM, and then re-enable it when the backup or restore is complete.

13.5.2.1 To restore server settings with the CCM on Windows

Context

You can use the Central Configuration Manager (CCM) to restore server settings. After you restore server settings, you must recreate your system's nodes on every computer in your system's cluster.

Procedure

1. Stop all the nodes on all of the computers in the cluster for which you are restoring server configuration settings by stopping the Server Intelligence Agent for each node.
2. Start the CCM on a computer that has a CMS.
3. From the toolbar, click *Restore Server Configuration*.
   The *Restore Server Configuration Wizard* appears.
4. Click *Next* to start the wizard.
5. When prompted, provide the port number for the temporary Central Management Server (CMS) to use, and the information to connect to the CMS system database, and click *Next* to continue.
6. Enter the cluster key, and click *Next* to continue.
7. When prompted, log on to the CMS by entering the CMS name and the user name and password of an account with administrative privileges, and click *Next* to continue.
8. Specify the location and name of the BIAR file that contains the server configuration settings you want to restore, and click *Next* to continue.
   A summary page displays the contents of the BIAR file.
9. Click *Next* to continue.
   A summary page displays the information you entered.
10. Click *Finish* to continue.
    A warning message indicates that existing server settings will be overwritten by values in the BIAR file, and if you proceed, the current server settings will be lost.
11. Click *Yes* to restore the server configuration settings.

The CCM restores the server configuration settings for the entire cluster from the BIAR file. Details of the restoration are written to a log file. The name and path of the log file appear in a dialog box.

12. If the restore operation failed, check the log file to determine the reason.
13. Click *OK* to close the wizard.

Results

The server settings from the BIAR file are restored on your system. Any nodes and servers existing in the BIAR file that did not exist on the system prior to the restore are created.

> **Note**
>
> Nodes and servers that existed on the system, but not in the BIAR file, are removed from the repository. The nodes and servers still appear in the CCM, but you can manually delete the `dbinfo` and `bootstrap` files for a node.

Next Steps

You must recreate the nodes in your system on each computer in the cluster.

Related Information

Using nodes [page 455]

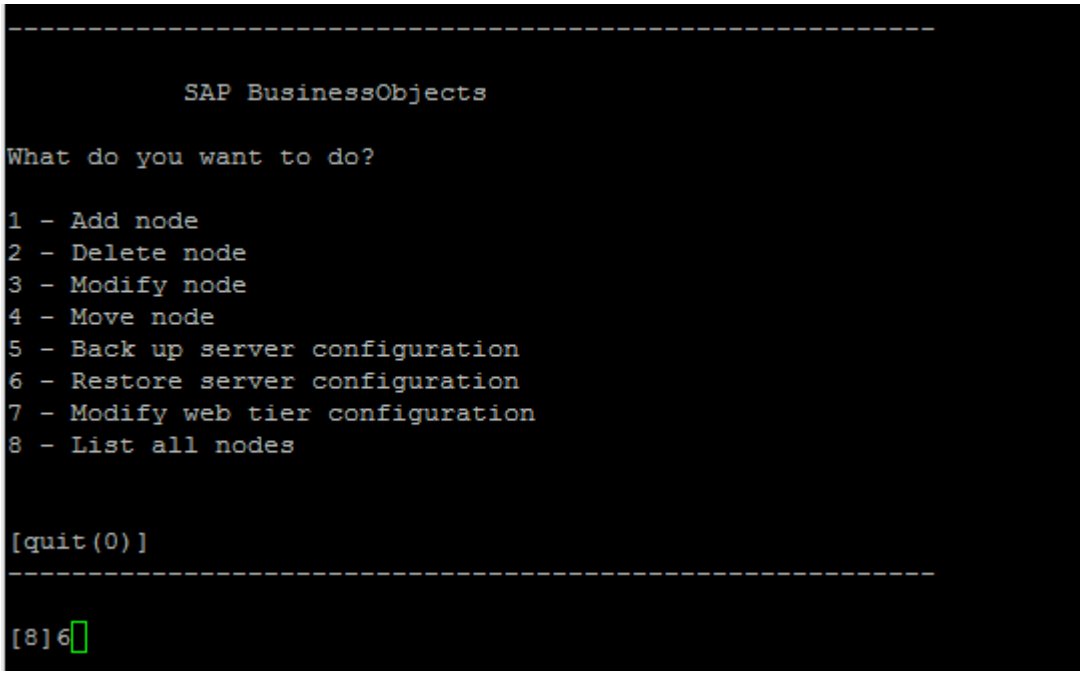
13.5.2.2 To restore server settings on Unix

Context

On Unix machines, use the `serverconfig.sh` script to restore your deployment's server settings from a BIAR file.

Procedure

1. Select *6 - Restore server configuration*, and press `Enter`.



2. Enter a port number for the temporary Central Management Server (CMS) to use, and press `Enter`.
3. On the next screens, specify the connection information to the CMS system database.
4. When prompted, log on to the CMS by specifying the system and user name and password of an account with administrative privileges, and press `Enter`.
5. When prompted, specify the location and name of a BIAR file that you want to restore the server configuration settings from, and press `Enter`.
   A summary screen displays the information that you have provided.
6. Verify that the information displayed on the screen is correct, and press *Enter* to continue.
   The `serverconfig.sh` script restores the server configuration settings for the entire cluster from the BIAR file that you specify. Details of the restore procedure are written to a log file. The name and path of the log file are displayed on the screen.
7. If the restore operation failed, check the log file to determine the reason.

13.5.2.3 To restore server settings with a script

Context

If you prefer, you can restore the server settings of your deployment by running the `RestoreCluster.bat` script on Windows, or the `restorecluster.sh` script on Unix.

On Windows, `RestoreCluster.bat` is located in the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` directory.

On Unix, `restorecluster.sh` is located in the `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts` directory.

Related Information

BackupCluster and RestoreCluster scripts [page 521]

13.5.3 Restoring BI content

If you've backed up Business Intelligence (BI) content to LCMBIAR files, you can use the promotion management tool to restore BI content, without restoring your entire system. For more information, see the “Promotion Management” chapter.

13.6 BackupCluster and RestoreCluster scripts

The following table describes the command-line parameters used with the `BackupCluster` script.

> ⓘ Note
>
> This script only backs up server settings for a cluster. Other data must be backed up separately.

BackupCluster parameters

Name	Description	Example
`-backup`	The name and path of the BIAR file that you want to back up your system's server settings to restore.	`-backup "C:\Users\Administrator\Desktop\my.biar"`
`-cms`	The host name of the machine where your system's Central Management Server is located. If your CMS is running on any other port than the default port, 6400, you must also specify the port number.	`-cms mycms:6400`
`-username`	The user name of an Administrator account.	`-username Administrator`
`-password`	The password of an Administrator account.	`-password Password1`

The following table describes the command-line parameters used with the `RestoreCluster` script.

RestoreCluster parameters

Name	Description	Example
`-restore`	The name and path of the BIAR file that contains the server configuration settings that you want to restore.	`-restore "C:\Users\Administrator\Desktop\my.biar"`

Name	Description	Example
`-username`	The user name of an Administrator account.	**`-username Administrator`**
`-password`	The password of an Administrator account.	**`-password Password1`**
`-displaycontents`	Displays a list of nodes and servers that the BIAR file contains.	**`-displaycontents "C:\Users\Administrator\Desktop\my.biar"`**

> **Note**
>
> Run the `RestoreCluster` script with the `-displaycontents` parameter to display the contents of the BIAR file before you restore the server settings.

The following parameters are required if you are backing up server settings from a system that is not running, or if you are restoring server settings.

Parameters used when using a temporary CMS

Name	Description	Example
`-usetempcms`	Creates a temporary CMS for the specified operation. After the operation is complete, the temporary CMS is stopped.	**`-usetempcms`**
`-cmsport`	The port number of the temporary CMS.	**`-cmsport 6700`**
`-dbdriver`	The database driver of the CMS system database. Accepted values are: • **`db2databasesubsystem`** • **`maxdbdatabasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`newdbdatabasesubsystem`** > **Note** > The **`newdbdatabasesubsystem`** parameter is for use with SAP HANA databases.	**`-dbdriver sqlserverdatabasesubsystem`**

Name	Description	Example
`-connect`	The CMS system database connection string.	`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"`
`-dbkey`	The cluster key.	`-dbkey abc1234`

Example

The following example shows how to back up your server settings to a BIAR file, using an existing CMS.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

Example

The following example shows how to display the contents of a BIAR file.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

Example

The following example shows how to restore your settings from a BIAR file. You must always use a temporary CMS when restoring server settings.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```

14 Copying Your BI Platform Deployment

14.1 Overview of system copying

This chapter describes how to create a duplicate of your BI platform deployment for testing, standby or other purposes.

For more information, see 1275068.

Related Information

Overview of backup and restore [page 499]

14.2 Terminology

Term	Definition
Source System	The original BI platform deployment.
Target System	The new deployment you want to create.
System Copy	The act of creating a duplicate of an existing BI platform deployment.
Homogeneous System Copy	The act of creating a duplicate system where the source and target systems have the same type of operating system and database. The BI platform supports only homogeneous system copying.
Heterogeneous System Copy	The act of creating a duplicate system where the source and target systems use different types of operating systems or databases but are based on the same data.
Database Copy	The act of creating a duplicate of the CMS system or auditing database using database vendor tools.

14.3 Use cases for system copying

The following table describes the goals you might want to achieve given the resources you might have, and directs you to the most appropriate solution.

Goal	Resources required	Solution
Goal: Identical copy I want to create a duplicate system for standby or testing with an identical hardware configuration and IP addresses/machine names.	• A target system with identical hardware to the source system, and • Backups of the source system or access to the source system to make a backup from.	Use the system backup and restore workflow detailed in this guide. See the Backing up the entire system [page 502] procedure. Recreate the target system from backups of the source system.
Goal: Copy I want to create a duplicate system for standby, testing, or training that has different hardware and IP addresses/ machine names from the source system.	• Source System (running or stopped) OR Backups of source system databases and files, and • Detailed system information described in To export from a source system [page 528]	Use the System Copy workflow, starting with Planning to copy your system [page 525], and follow the instructions for the rest of the chapter. **Note** You can create your target system on a computer with an existing BI platform deployment of the same release, support package, and patch level, or a clean computer with no BI platform installed.

Related Information

Backups [page 502]
Planning to copy your system [page 525]

14.4 Planning to copy your system

A system copy does not have to reflect your current system. You can create a copy of your system and wait some time before proceeding to recreate the copy on the target system, or you can use a previous backup of the source system as the base for your target system. This will mean that the copy will be of the system as it was at the time the copy was created. For example, if you wait one month, the copy will recreate the system as it was one month ago.

After reviewing the use cases in the preceding section and deciding which one best suits your needs, you should develop a system copy plan.

Create a system copy plan

When planning to copy a system, you should decide the following in advance:

- Will the source system will be stopped or active while the copy is being made? (The procedure can be done under either circumstance.)

    - If the source system is stopped, how much downtime will be required?
    - Plan some time for testing to ensure the integrity of the target system.
- Which database tools you want to use for database backup and restoration.
- Which machines the target system will be deployed on, and where each node will be hosted.
- Which optional components you want to copy.
- The database type to use for the target CMS database, and any other optional databases you will be copying.

You should also give consideration to the following:

- Which BI platform components your source system has installed. You can use the *Add/Remove* > *Modify* function of the installation program to view the list of currently installed components.
- If the target system is installed on a different hardware setup from the source system, may need to tune the target system for better performance. See the information about improving your system performance in the *SAP BusinessObjects Business Intelligence sizing companion guide*.
- You may want the target system to report from reporting databases other than the source system databases. In this case you will need to change the database connection information for the reporting databases. You can do this by keeping the same DSN name but pointing to DSN on the target system to another database.

Required source system components

- CMS system database
- FRS file store
- Semantic layer configuration files
- Auditing database (optional)
- Monitoring database (optional)
- Promotion management Subversion database (optional)

14.5 Considerations and limitations

You should be aware of the following considerations when making a copy of your BI platform deployment.

Area	Consideration
SAP Business Warehouse integrations	If you are using the BI platform and SAP ERP or BW in an integrated environment, before copying your system, read the SAP system copy documentation. The system copy guides are available at http://www.sdn.sap.com/irj/sdn/systemcopy (SMP login required). Choose your SAP NetWeaver version; the relevant copy guides can be found in the installation guides folder.

Area	Consideration
Program version	The source and target systems must be at the same version, support package, and patch level.
Content and configuration settings	Only the entire source system can be copied. You cannot selectively copy content or system configuration settings.
Installation path	The installation path on the source and target locations must be identical: for example, if you installed the source system to `C:\SAP BusinessObjects Enterprise XI 4.0`, you must install the target to `C:\SAP BusinessObjects Enterprise XI 4.0`.
Host operating system	The source and target operating systems must be the same.
CMS database software type	CMS source and target databases must be of the same type. You will have the option of changing to another supported database type after copying the system.
Auditing database software type	If you are copying auditing data, the auditing source and target databases must be of the same type. After the copy has been created, you can establish a new database of a different type. **Note** If you establish a new database, existing events will not be copied to that database, only new events will be recorded to the new database.
Web tier customization	The copy procedure will not copy web tier components from the source system. If you customized the web tier (modified `.properties` files in the `custom` folder, for example) you must manually apply those customizations to the target.
Topics not covered by these instructions	This workflow does not describe how to export or import a database. Use your database vendor tools for database copying and restoring.

The following data will be copied during the system copy procedure:

- The CMS repository database. (contains reports, analytics, folders, rights, users and user groups, server settings, and other BI content and system content)
- The Auditing database. (contains auditing events triggered by BI platform servers or client applications)
- The Monitoring database. (contains trending data from metrics, probes, and watches)
- The Version Management database. (contains different versions of reports, analytics, other BI resources, and version information)

  Note

  For a description of the databases and their contents, see the Databases [page 34] section of this guide.

- Semantic layer configuration files

Web tier configuration, search index, and any data not specifically mentioned above are not copied.

Considerations for file recovery copies

If you are copying a system for the specific purpose of recovering a file that was accidentally deleted, you should be aware of the following additional considerations:

Using your backup, perform the steps in the procedure To import to a target system [page 532] on the production system.

- Do not install all nodes, just install the first node which will contain the CMS and its database.
- Do not install auditing, Promotion Management, or monitoring databases.
- Do not recreate connections to the auditing or reporting databases.

Use LCM to promote the object you want to recover from the target system to the source system.

14.6 System copy procedure

The following procedures guide you through the two stages of copying your BI platform deployment.

14.6.1 To export from a source system

Prerequisites

You will need to make note of the following information from the source system. If you want to write this information down there is a worksheet you can use at System copy worksheet [page 1122].

Property	Location
The CMS cluster key (make sure to keep the record secure).	Created by the system administrator when the BI platform was installed.
The name of the nodes.	Go to the *Servers* tab of the CMC, on the left tree expand *Nodes*.
The machine name and the BI platform installation folder for each machine in the deployment.	Go to the *Servers* tab of the CMC, right-click the CMS and select *Placeholders*. Look for the value of the `%INSTALLROOTDIR%` placeholder.
The BI platform administrator password (make sure to keep the record secure).	Created by the system administrator when the BI platform was installed.
All database connections that might be used by the CMS, and the user names and passwords associated with those connections. This can include auditing database if you want	Go to the *Servers* tab of the CMC, right-click the CMS and select *Metrics*. Look for the following metrics:

Property	Location
to copy this information. Make sure to get this information for all machines in the cluster. **Note** If you are copying the auditing database, you also need the auditing database connection names and credentials.	• *System Database Connection Name* • *System Database Server Name* • *System Database User Name* • *Data Source Name* • *Auditing Database Connection Name* (optional) • *Auditing Database User Name* (optional)
For every machine in the cluster, the details (client types, versions) of any other database connections (used by universes and reports for example). Make sure to include user names and passwords.	For Crystal reports that report directly from databases, look at the connection information using the SAP Crystal Reports 2025 or SAP Crystal Reports for Enterprise designers. For universe connection information, use Information Design Tool (.unx).
The version, support package, and patch level of the source system.	On Windows this can be determined by looking at the *Remove or Change* programs tool. On Unix, you can use the `modifyOrRemoveProducts.sh` utility in the BI platform installation directory.
The file store locations for every Input FRS and Output FRS in the deployment.	Go to the *Servers* tab of the CMC, right-click the Input or Output FRS and select *Properties*. Look for the *File Store Directory* property. **Note** If the value begins with % then this is a placeholder, and you will need to click on *Placeholders* and make a note of the directory listed under that placeholder.
If you plan to copy Promotion Management, the location of the Promotion Management database folder and Subversion folders.	The default folder for the Promotion Management database in Windows installations is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride` and on Unix it is `<INSTALLDIR>/sap_bobj/data/LCM/LCMOverride`. The default locations for the Subversion files in Windows installations are: • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository` and on Unix they are:

Property	Location
	• <INSTALLDIR>/check_out (This directory is created only after you have used Subversion to check out files.) • $HOME/LCM_Repository
If you plan on copying the monitoring database, the monitoring database folder.	This is set in the CMC. Go to the *Applications* management area of the CMC, Select *Monitoring Application* *Properties* and look for the *Trending database backup directory*. The default folder in Windows installations is <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB and on Unix it is <INSTALLDIR>/sap_bobj/Data/TrendingDB.
The semantic layer folder path.	The default folder path in Windows installations is <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\ by default.

After you've recorded the information above:

Procedure

1. Use your database vendor backup tools to create a backup copy of the following databases:
   - The CMS system database
   - The auditing database (optional)
2. Using file backup tools, back up the following sets of files:
   - The FRS input and output file stores.
   - The monitoring trending database (optional). This can be achieved by backing up files from the monitoring folder as recorded on the worksheet. By default, on Windows it is: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. On Unix: <INSTALLDIR>/sap_bobj/Data/TrendingDB.
   - Configuration files from the semantic layer folder: the `cs.cfg` file in the `connectionServer` folder, and any `.sbo` and `.prm` files in any of its subfolders.

     > **Note**
     >
     > For constraints and a detailed description of this workflow, please see the Hot backups [page 503] section.
3. The following files are user-customizable. If you have customized any of them, back up the files from the source system, and later restore them to the same folder on the target system:

- `BO_trace.ini` installed to:
  - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
- `clientSDKOptions.xml` installed to:
  - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
  - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
  - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
- `CRConfig.xml` installed to:
  - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
- `mdas.properties` installed to:
  - `[INSTALLDIR]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
- WDeploy configuration files installed to `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf`:
  - `config.apache`
  - `config.jboss7`
  - `config.sapappsvr75`
  - `config.tomcat6`
  - `config.tomcat7`
  - `config.weblogic11`
  - `config.websphere7`
  - `config.websphere8`
  - `wdeploy.conf`

4. The following web-tier files are user-customizable. If you have made changes to any of these files, back up the files from the source system. Later, you will need to restore these files or reapply the changes to the target system.
   - `BO_trace.ini` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
   - `clientaccesspolicy.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
   - `clientSDKOptions.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
   - `crossdomain.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
     - `[INSTALLDIR]tomcat/webapps/ROOT`
   - Any customized files in the `config/custom` folder (in the web tier). Back up these files to transfer the customization to the target system.

5. Back up any custom extensions that you've manually added to the source system; for example, publication extensions, custom libraries, and so on.

Next Steps

Keep the information recorded above with the copy of the databases and files. You may want to keep a second copy which you can update as required for future system copy procedures.

14.6.2 To import to a target system

Prerequisites

This procedure assumes you have created backup copies of the source deployment databases and system files you want to use in your target system. All backup files must be from the same backup set. You will also need the details (cluster key and database credentials for example) noted in "To export from a source system".

If the target system will reside in a network location with access to the source system resources, you should ensure the target system does not attempt to access those resources until it has been reconfigured. This can be accomplished by placing a firewall between the target system and the source system resources, or leaving the source system stopped while you start the target system. After the first time you start the target system, the firewall can be removed or the source system can be started.

If the target system already has the BI platform installed, ensure it is at the same version, support package, and patch level as the source system at the time the copy was created. Also ensure it uses the same installation path as the source system.

Procedure

1. On the target system, create the connections to the database or databases where you intend to put the CMS repository, auditing database, and reporting database.

   > ⓘ Note
   >
   > While the connections can point to a different database, they must have the same connection name or DSN and use the same credentials as the source system.

2. Use your database tools to restore the CMS system database and the auditing database (if required) from the source-system backup to the target database.

   If the universes or reports on the target system need to use a different reporting database, modify the database connection to point to that database.

   If you require further instructions on this step, see the Restoring your system [page 509] topic.

3. If the BI platform is installed on the target host system, skip to Step 4. If the BI platform is not installed, install the BI platform on the target host system keeping the following steps in mind:

a. Install the same program version, support package, and patch level as the source system.
b. Use the same installation path as the source system.
c. Select the same components that were installed on the source system.
d. When the installation program asks you to create the CMS database (and auditing database if applicable), choose the *Use an existing database server* option and enter the connection name and credentials set up in step 1.

> **Note**
>
> Do not choose to reinitialize the CMS database.

e. When prompted for the *Node Name*, use the same names, port numbers, platform administrator password and cluster key as the source system.

   For complete installation instructions, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. When the system has finished installing, go to step 6.

> **Note**
>
> If you are not copying your auditing data from the source system, you can create a new auditing database by configuring auditing during the installation procedure.

f. Stop all nodes in the CCM.

4. If the BI platform is already installed on the target system, stop all nodes in the CCM. On the target system CMS host computer, start the CCM.
5. If the BI platform is already installed, add a new node, using the *Recreate Node* option.
   a. Use the *Node Name* and *SIA Port Number* from the source system.
   b. Choose to *Start a new temporary CMS*.
   c. Select a new *CMS Port Number* (can be any free port) and *CMS Database Type* (matching the restored database type).
   d. Enter details for the connection the CMS database was restored to in Step 1.
   e. Enter the cluster key from the source-system.
   f. Enter the Administrator password from the source system.
6. Restore the Input and Output FRS file stores to the target system file store. Use the same folder as was used on the source system.
7. Restore the monitoring database folder (if you want to copy monitoring information) to the same folder as was used on the source system.
8. Restore the Promotion Management database folder (if you want to copy Promotion Management information) to the same folder as was used on the source system.
9. Restore the Subversion files (if you want to copy Promotion Management information) to the same folder as was used on the source system.
10. Restore the semantic layer/connection configuration server files to the same folder as was used on the source system.
11. Restart the target system host computers.
12. If you installed the BI platform on the target system in step 3, apply any support packages or patches required to match the source system.
13. If the target system will run on multiple host computers, repeat steps 1–11 for each host computer.

    Use the Expand install option when installing additional BI platform nodes, and keep in mind that the same node names as the source system should be used for the additional nodes in the target system.

14. If the target system CMS database will use a different database type from the source system, use the CCM to perform Copying data from one CMS system database to another [page 495], specifying as destination the database you want to use for the copy.
15. Restore any user-customizable files that you backed up in step 3 of the procedure "To export from a source system".
16. Restore any web-tier files that you backed up in step 4 of the procedure "To export from a source system".

    "Web tier" refers to the WDeploy staging area where you can perform your customizations, and to the web-tier content that is deployed to the application server.

    When applying changes to the target system, do not apply changes to the application server directory; apply the changes to the WDeploy staging area, and then redeploy the web tier to the application server using WDeploy.

    The WDeploy staging area is this location on Windows: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/warfiles`.
17. Restore any extensions that you backed up in step 5 of the procedure "To export from a source system".

Next Steps

After the system copy of the BI platform is performed:

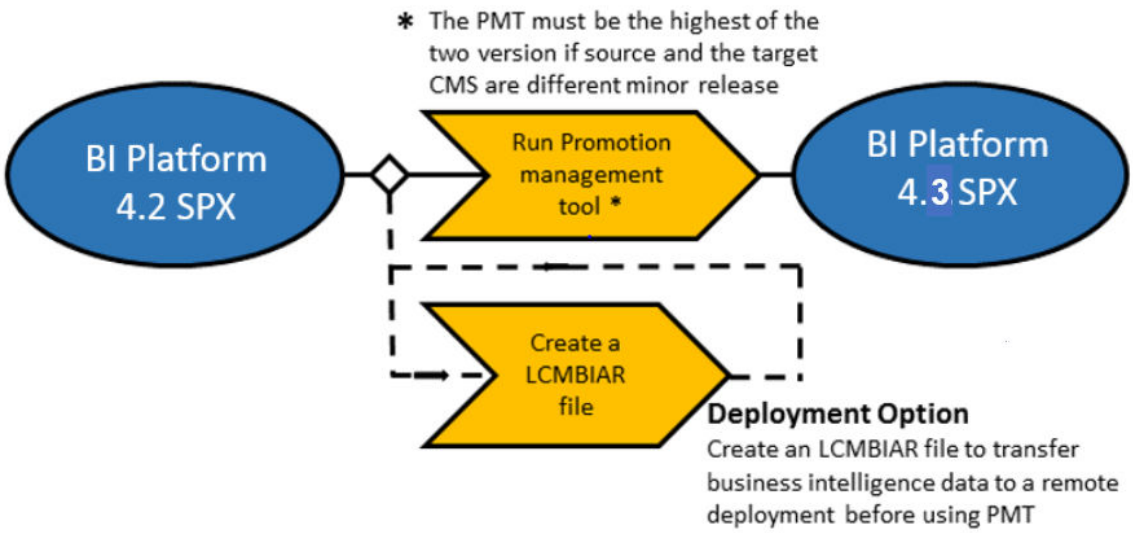
1. The installation of the first node on the target creates a temporary CMS, which will be stopped at the end of the installation. Using the CMC, go to the Servers page and delete this CMS.

   > → Remember
   >
   > If you do not remove the source system (or if you use it concurrently with the target system), renaming the cluster on the target system is recommended.
2. Run the Repository Diagnostic Tool on the target CMS database.
3. If applicable, configure Windows AD single sign-on (SSO) on the target system. See SSO to the BI platform with AD authentication [page 303].
4. If applicable, configure SLD on the target system. For details, see SAP Note 1508421: "SAP SLD Data Supplier for Apache Tomcat".
5. Perform a sanity check on the target system to ensure its integrity.
6. Perform a full search re-index.

15 Promotion Management

15.1 Welcome to promotion management

15.1.1 Overview



The promotion management tool allows you to:

- Move or transport business intelligence (BI) resources from one repository to another.
- Manage dependencies of the resources.
- Roll back the promoted resources at the destination system, if required.

The promotion management tool also supports the management of different versions of the same BI resource.

The promotion management tool is integrated with the Central Management Console. You can promote a business intelligence resource from one system to another only if the same version of the BI platform is installed on both the source and destination systems.

15.1.2 Features

The promotion management tool allows you to perform the following actions on infoobjects in the destination desployment.

- Create a new job

- Copy an existing job
- Edit a job
- Schedule a job promotion
- View the history of a job
- Export as LCMBIAR
- Import both BIAR /LCMBIAR

The promotion workflow also includes the following tasks:

- *Managing Dependencies* This feature allows you to select, filter, and manage the dependents of the infoobjects in the job that you want to promote.
- *Scheduling* This feature allows you to specify a time for job promotion, rather than promote a job as soon as it is created. You can specify the job promotion to run once or on a recurring schedule.
- *Security* This feature allows you to promote infoobjects along with the associated security rights and if required promotes infoobjects associated with application rights.
- *Test Promotion* This feature allows you to check or test the promotion to ensure that all the preventive measures are taken before the actual promotion of the infoobjects.
- *Rollback* This feature allows you to restore the destination system to its previous state, after a job is promoted. You can roll back an entire job or a part of the job.
- *Auditing* The events generated by the promotion management tool are stored in the audit database. This feature enables you to monitor the events that are logged in the audit database.
- *Promotion Management Override Settings* This feature allows you to scan and promote the overrides through a job promotion.

15.1.3 Application access rights

This section describes the application access rights for the promotion management tool.

- You can set access rights to the promotion management tool within the CMC.
- You can set granular application rights to various functions within the promotion management tool.

To set specific rights in the promotion management tool, complete the following steps:

1. Log on to the CMC and select *Applications*.
2. Double-click *promotion management*.
3. Click *User Security*, and select a user. You can view or assign security rights for the user.
4. The following promotion management specific rights are available:
    - Allow access to edit overrides
    - Allow access to Include Security
    - Allow access to administration
    - Allow access to Manage Dependencies
    - Create Job
    - Delete Job
    - Edit Job
    - Edit LCMBIAR
    - Export as LCMBIAR

- Import LCMBIAR
- Promote Job
- Rollback Job
- View and Select BOMM (BusinessObjects Metadata) Objects
- View and Select Business Views
- View and Select Calenders
- View and Select Connections
- View and Select Profiles
- View and Select QaaWS
- View and Select Report Objects
- View and select Security settings
- View and select Universes

5. If you wish to assign rights to a selected user, select the appropriate right and click *Assign Security*.

The promotion management tool access rights are set within the CMC.

15.1.4 Support for WinAD in promotion management

In order for the promotion management tool to function properly, you must add the following to all `javaargs` arguments for all Adaptive Job Servers:

```
Djava.security.auth.login.config=<path>\bsclogin.conf,Djava.security.krb5.conf=<path>\krb5.ini
```

> → Remember
>
> Specify the correct path to `bsclogin.conf` and `krb5.ini` on your deployment.

15.2 Getting started with the promotion management tool

15.2.1 Accessing the promotion management tool

Context

To access the promotion management tool, select *Promotion Management* from the CMC home page.

Results

Any user with view permissions to the *Promotion Jobs* folder can launch the promotion management tool. However, to create, schedule, or promote a job, the user must be granted additional rights by the administrator.

15.2.2 User interface components

This chapter discusses the GUI components in the promotion management tool.

- Promotion management workspace toolbar
- Workspace panel
- Tree panel
- Details panel
- Shopping Cart and Job Viewer page

Promotion management workspace toolbar

The following table lists the options included in the promotion management workspace toolbar and discusses the tasks you can perform using these options:

Option	Description
	Allows you to create a new folder. The new folder is created as a subfolder in the *Promotion Jobs* folder.
	Allows you to copy and remove the selected job or folder from its current location.
	Allows you to copy the job or folder from its current location.
	Allows you to paste the copied job or folder in a new location.
	Allows you to delete an existing job or folder.
	Allows you to refresh the home page, to obtain the updated list of jobs or folders.
Properties	Allows you to modify the properties of the selected job. You can modify the title, description, and keywords of the selected job.
History	Allows you to view the history of the selected job.
New Job	Allows you to create a new job.
Import	Allows you to import a BIAR, LCMBIAR, or Override files.
Edit	Allows you to edit the selected job.
Promote	Allows you to promote the selected job.

Option	Description
Rollback	Allows you to undo the promoted job on the destination system. **Note** If the job promotes objects to the destination, rollback will delete these objects. If the job updates objects on the destination, rollback will restore the previous version of the objects.
	Allows you to navigate between pages of a job list. You can use this option to navigate a single page, or navigate to a specific page by entering the relevant page number.
Search	Allows you to search for specific jobs. You can search for a job by its name, keywords, description, or all three parameters.
Promotion Jobs	Allows you to view the jobs and folders.
Promotion Status	Displays the promoted jobs according to their status, such as Success, Failure, or Partial Success.

Workspace panel

The Workspace panel in the promotion management home page displays the list of jobs. You can use this panel to view the name, status, creation time, and last run time of the job, the source and destination systems, and the job creator.

Tree panel

The Tree panel in the promotion management home page displays the tree structure, which includes the *Promotion Job* folder and the *Promotion Status* folder. The jobs are displayed in a hierarchical structure under the *Promotion Job* folder. The *Promotion Status* folder displays the promoted jobs according to their status.

Job Viewer page

The “Job Viewer” page is displayed when a user creates a new job or edits an existing job. It contains a dynamically-generated list of infoobjects to be promoted and a details panel. The list categorizes the infoobjects into user groups, universes, and connections. The details panel shows the contents of the node selected from the list.

15.2.3 Using the Settings option

Context

The Settings option allows you to configure settings before promoting infoobjects from one BI platform deployment to another BI platform deployment and SAP deployment. This section describes how to use the settings options.

Click the *Settings* drop-down in the *Promotion Jobs* screen. This drop-down displays the following options:

- *Manage Systems* This option allows you to add all the systems required for promotion management activities.
- *Rollback Settings* This option allows you to select a system for which rollback is enabled.
- *Job Settings* This option allows you to view completed instances onthe Dependencies page and allows managing job instance cleanup activities. It also allows filtering by job creation date.
- *CTS settings* This option allows you to add the web service and SAP BW system information for the Enhanced Change and Transport System integration.

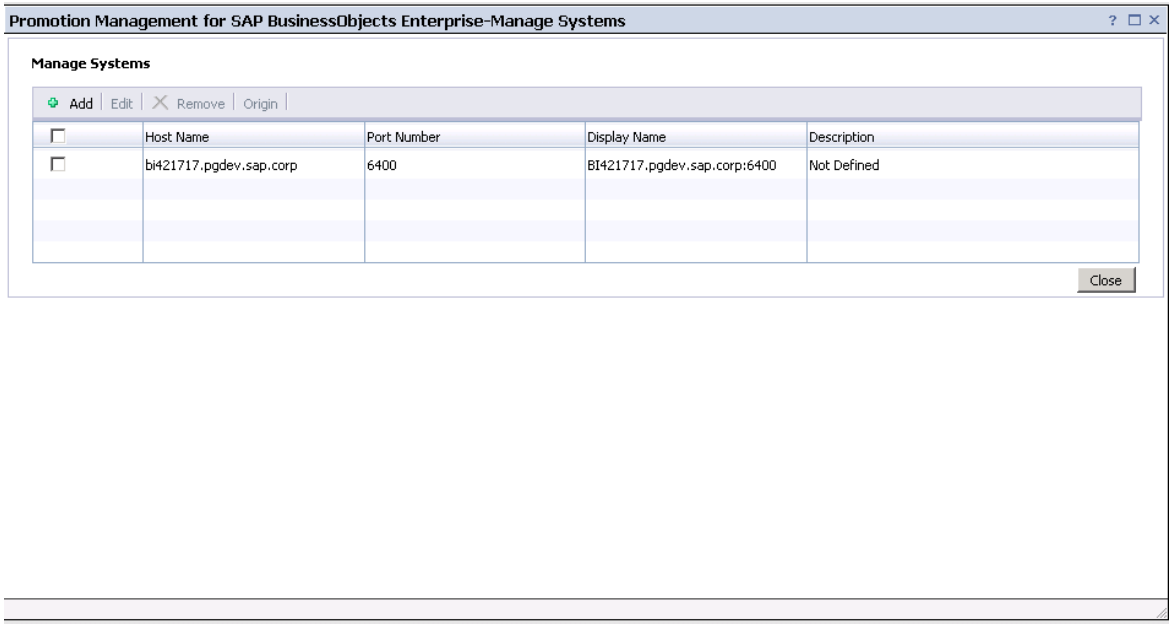
15.2.3.1 To use the Manage Systems option

Context

This section describes how to use the Manage Systems option. You can add or remove host systems using this option.

To add a host system, complete the following steps:

1. On the promotion management workspace toolbar, click *Settings* and then click *Manage Systems*.
   The *Manage Systems* window is displayed. This window displays a list of host names, port numbers, display names, and descriptions.



2. Click *Add*.
   The *Add System* dialog box is displayed.
3. Add the host name, port number, display name, and the description in the appropriate fields.

   > **Note**
   >
   > Select the *Mark as 'Origin'* option to identify the system as a source system (the system where the connection information originated from). This option is useful for working with overrides.

4. Click *OK* to add the system.
   The host system is added to the list.

> **Note**
>
> To remove or edit a host system, select a host system and click *Remove* or *Edit*.

Related Information

To use the Rollback Settings option [page 541]
To use the Job Settings option [page 542]

15.2.3.2 To use the Rollback Settings option

Context

By default, the rollback process is enabled at the system level. The *Rollback Settings* option allows you to disable the rollback process at the system level.

To disable the rollback process at the system level, complete the following steps:

1. In the *Rollback* window, from the list of host systems, select the host system to disable the rollback process.
2. Click *Save and Close* to save the modifications.

Related Information

To use the Job Settings option [page 542]

15.2.3.3 To use the Job Settings option

Context

The Job Settings option allows you to specify whether you want to show completed instances on the "Manage Dependencies" page and the number of job instances that can exist in the system. You can specify one of the following options:

- *Show completed instances in Manage Dependencies page* This option allows viewing completed instances on the "Manage Dependencies" page that can be added to the job.
- *Delete Instances when more than N instances of a Job* This option allows specifying the maximum number of job instances per job in the system.
- *Delete Instances after N days for the Job* This option allows specifying the job instances created before a specified number of days to be deleted.
- From the *Show Jobs Created* list, you can select the time interval to view the jobs created during the specified period.

To set the *Job Settings* option, complete the following steps:

1. Select the option, and enter the preferred value.
2. Click *Save* to save the updated changes.

You can click *Default Settings* to set the default values, and you can click *Close* to close the window.

> ⓘ Note
>
> The old job instances are deleted only when the job is executed the next time.

15.2.3.4 Using the Override Settings option

The Override Settings option allows promoting overrides using a job promotion or an LCMBIAR file. This option allows scanning, promoting, and editing the database connection information for Crystal Reports and Universe connections. You can also use it to edit the QAAWS URLs.

> ⓘ Note
>
> To use the Override Settings option, you must install Adobe Flash Viewer.

The term *system* is used in the following procedures. There are three types of systems:

- *Origin*: The originating system for any connection information.
- *Central Promotion Management*: The system which runs the Promotion Management tool.
- *Destination*: The end system to which the BI resources are promoted.

15.2.3.4.1 To promote overrides

Prerequisites

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 540].

Context

To promote the overrides, complete the following steps:

Procedure

1. On the promotion management workspace toolbar, click the *Override Settings* option.
   The *Override Settings* window is displayed.
2. In the *Origin* pane, select the desired source system from the drop-down menu.

   > ⓘ Note
   >
   > You can also choose to log in to a *New System*. In order to choose a new system as the source system, perform the following:
   >
   > 1. Select *New System* from the drop-down menu.
   >   The Origin Login dialog box appears.
   > 2. Enter the valid credentials in the *System*, *Username*, *Password*, and *Authentication* fields.
   > 3. Choose *Log On*.
3. Choose *Login*.
4. Choose *Scan Now*.

   The scanning process starts. The *list of unique connections* is displayed.

   > ⓘ Note
   >
   > To schedule a recurring scan, choose *Recurrence Settings*.
5. In the list of overrides, select the overrides that you want to promote by checking the checkboxes corresponding to each override.

   > ⓘ Note
   >
   > You can search for overrides from the list of overrides by using keywords like override name, last updated date, etc.
   >
   > You can also Filter overrides by the following parameters: All, Connection, Qwaas, Crystal Report.
   >
   > Additionally, you can sort overrides in alphabetical order.

6. In the *Destination* pane, select the desired Destination system from the drop-down menu. You can specify multiple destination systems.

   > **Note**
   >
   > You can also choose to log in to a *New System*. In order to choose a new system as the destination system, perform the following:
   > 1. Select *New System* from the drop-down menu.
   >   The Destination Login dialog box appears.
   > 2. Enter the valid credentials in the *System*, *Username*, *Password*, and *Authentication* fields.
   > 3. Choose *Log On*.

   To export the overrides as an LCMBIAR file, perform the following:
   1. Select Export to LCMBIAR File from the drop-down menu.
   2. Choose *Export*.
      The *Export Settings* dialog box appears.
   3. Enter valid credentials in the respective fields.
   4. Choose *Done*.
7. Choose *Promote*.

   The Multiple Destination Overrides dialog box appears.

   > **Note**
   >
   > By default, all the destination systems that you are currently logged into are selected. You can choose to selectively promote overrides to a particular destination system by checking the checkbox that corresponds to the desired destination system.

8. Choose *Done*.

   The promotion of overrides is complete.
9. Login to one of the destination systems using valid credentials.

   A list of all the promoted objects is displayed in a list of unique connection. The status of these objects is Inactive.
10. Choose *Update* for the objects you want to edit.

    The *Edit Common Connection Properties* dialog box appears.
11. Update the required values, and choose *Done*.

    The status of the edited objects becomes Active.

    > **Note**
    >
    > You can also activate a connection by choosing *Inactive*, without the need to edit the connection in the Destination system.

12. Choose *Save*.

15.2.3.4.2 To promote overrides using BIAR Files

Prerequisites

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 540].

Context

To promote the overrides through BIAR files, complete the following steps:

Procedure

1. On the promotion management workspace toolbar, click the *Override Settings* option.
   The *Override Settings* window is displayed.
2. If you are logged on to the Central Promotion Management system, log out from the system.
3. Click *Login* to connect to the Origin system.
   The *Login to system* window is displayed.
4. In the *Override Settings* screen, select the source system marked as *Origin* to scan the objects and login to the system using valid credentials.
5. From the *Start* drop-down list next to *Scan*, select the *Start* option.
   The scanning process starts.The List of Overrides is displayed.

   > ⓘ Note
   >
   > To schedule a recurring scan, select *Recurrence Settings* option from the drop-down list.

6. In the list of overrides, change the status of the required objects to Active, and click *Save*.
7. Click *Promote Overrides*.
   The *Promote Overrides* screen is displayed where the list of destination systems is displayed.
8. To encrypt the BIAR file using a password, click *Password Encryption* checkbox.
   The *Password* and *Confirm Password* fields are enabled.
9. Enter a password in the *Password* field. Re-enter the same password in the *Confirm Password* field.
10. Click *Export*, and save the overrides BIAR file to a file system.
11. Log into the destination system through the CMC, and in the promotion management tool click *Import* > *Override File*.
    The *Import LCMBIAR file* window is displayed.
12. Click *Browse* to browse the BIAR file.
13. Enter the password of the BIAR file in the *Password* field.

    > ⓘ Note
    >
    > The *Password* field is displayed only if the BIAR file you selected is encrypted using a password

14. Click *OK*. The promotion of overrides is complete.
15. Log off from the origin system.
16. From the *Override Settings* screen, click *Login*.
    The *Login to system* window is displayed.
17. Login to the destination system using valid credentials.
    A list of imported objects is displayed in List of Overrides.The status of these objects is Inactive.
18. Click the *Select* check box for the objects you want to edit, and click *Edit*. The edited objects are indicated by an icon.

    > ⓘ Note
    >
    > You can delete the override objects by clicking on the icon.

19. Update the required values, and click *Done*.
    The state of the edited objects becomes Active.
20. Click *Save*.

15.3 Using the promotion management tool

When you launch the promotion management tool, by default, you are taken to the *Promotion Jobs* page.

> ⓘ Note
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

The *Promotion Jobs* home page screen includes various tabs that enable you to perform the following tasks:

- Click *New Job* to create a new job. You can also right-click the home page screen and select *New Job* from the list.
- Click *Import* > *Import file* to import a BIAR file or LCMBIAR directly from the file system, instead of performing the entire procedure of creating a new job.
- Click *Import* > *Override File* to import overrides.
- Select an existing job from the list and click *Edit* to edit the selected existing job.
- Select an existing job from the list and click *Promote* to promote the job from the source system to the destination system, or export the job to an LCMBIAR file.
- Select an existing, previously-run job from the list and click *Rollback* to revert the promoted objects from the destination system.
- Select an existing, previously-run job from the list and click *History* to view the previous promotion instances of the selected job.
- Select an existing job from the list and click *Properties* to view the properties of the selected job, such as title, ID, file name, and description.

The *Promotion Jobs* application area displays the list of jobs and folders that exist in the system, along with the following information for each job or folder:

- *Name:* Displays the name of the job or folder that was created.

- *Status:* Displays the status of the job, such as Created, Success, Partial Success, Running, or Failure.
- *Created:* Displays the date and time when the job or folder was created.
- *Last Run:* Displays the date and time when the job was last promoted.
- *Source System:* Displays the name of the system from which the job is promoted.
- *Destination System:* Displays the name of the system to which the job is promoted.
- *Created By:* Displays the name of the user who created the particular job or folder.

> **Note**
>
> The promotion management tool uses the BI platform SDK for all of its activities.

15.3.1 Creating and deleting folders

This section describes how to create and delete a folder in the promotion jobs home page.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

15.3.1.1 To create a folder

This section describes how to create a folder.

To create a folder, complete the following steps:

1. In the promotion management toolbar, click .
2. In the *Create Folder* dialog box, enter the folder name.
3. Click *OK*.

A new folder is created.

Related Information

To create a job [page 548]
To delete a folder [page 547]

15.3.1.2 To delete a folder

This section describes how to delete a folder.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To delete a folder, complete the following steps:

1. Select a folder in the *Promotion Jobs* home page.
2. Click .
   The confirmation dialog box is displayed.
3. Click *OK*.

The selected folder is deleted.

Related Information

To create a job [page 548]

15.3.2 To create a job

This section describes how to create a new job by using the promotion management tool.

The following table discusses the GUI elements and fields that you can use to create a new job:

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

Field	Description
Name	Name of the job that you want to create.
Description	Description of the job you want to create.
Keywords	The keywords for the contents of the job you want to create.
Save Job in	The default selected folder is displayed.
Source System	The name of the BI platform system from which you want to promote a job.
Destination System	The name of the BI platform system to which you want to promote a job.
User name	The login ID that you must use to log into the source or destination system.
Password	The password that you must use to log into the source or destination system.

Field	Description
Authentication	The authentication type that is used to log into the source or destination system. The promotion management tool supports the following authentication types: • Enterprise • Windows AD • LDAP • SAP

> **Note**
>
> Prior to job creation, ensure that the overrides, if any, have been edited and updated in the destination system so that the BI platform content is automatically updated. For more information see, Using the Override Settings Option.

To create a new job using the promotion management tool, complete the following steps:

1. Launch the promotion management tool.
2. In the *Promotion Jobs* home page, click *New Job*.
3. Enter the name, description, and keywords for the job in the appropriate fields.

   > **Note**
   >
   > Providing information in the Description, Keywords, and Destination System fields is optional.

4. In the *Save Job in* field, browse and select the folder in which you want to save the job.

   > **Note**
   >
   > By default, the *Save Job in* field will be populated by the name of the folder highlighted in the folders pane prior to clicking *New Job*.

5. Select source system and destination system from the respective drop-down lists.
   If the name of the system is not included in the drop-down list, click the *Login to a new CMS* option. A new window is launched. Enter the name of the system along with the user name and password.
6. Click *Create*.
   The “Add Objects” window is displayed.
7. Select the objects from the source system to be added to the job, and then click *Add & Close*.
8. Click *Save*.

The newly created job is stored in the CMS repository of the source system.

> **Note**
>
> If you create a job with a folder as the primary object and the job is a recurring one, the job will include any content added to the folder at the next run-time.

Related Information

Using the Override Settings option [page 542]

15.3.2.1 To log onto a new CMS

Context

This section describes how to log into a new CMS.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To log into a new CMS, complete the following steps:

Procedure

1. Launch the promotion management application.
2. Create a new job.
   For more information on creating a new job, see To create a job [page 548].
3. From the *Source System* drop-down list, select *Login to a New CMS*.
   The *Login to System* dialog box is displayed.
4. Select the system from the drop-down list or type in a new system name.
5. Enter the user credentials, select the appropriate authentication type, and click *Login*.
6. From the *Destination System* drop-down list, select *Login to a New CMS*.
7. Select the system from the drop-down list or type in a new system name.
8. Enter the user credentials, select the appropriate authentication type, and click *Login*.

Related Information

To edit a job [page 552]
To add an infoobject to a job [page 553]
To promote a job when repositories are connected [page 556]
To schedule a job promotion [page 563]

15.3.3 To create a new job by copying an existing job

Context

This section describes how to create a new job by copying an existing job.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To create a new job by copying an existing job, complete the following steps:

1. Launch into the promotion management tool.
2. In the *Promotion Jobs* home page, click *New Job*.
3. Click the *Copy an Existing Job* option.
   The *Copy an Existing Job* window is displayed displaying the list of jobs in the *Promotion Jobs* folder.
4. Select the required job from the list, and click *Create*.
   The name, keywords, and description of the job, as well as the *Save Job In* and *Destination* fields are displayed. You can modify these fields as necessary.
5. In the *Save Job in* field, browse and select the folder in which you want to save the job, and click *Create*.

A new job is created, and the *Add Objects* window is displayed.

Related Information

To add an infoobject to a job [page 553]
To edit a job [page 552]
To promote a job when repositories are connected [page 556]

15.3.4 To search for a job

The search feature in the promotion management tool allows you to locate a job that is available in the repository.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To search for a job, complete the following steps:

1. In the *Search* field of the home page, enter the text that you want to locate.
2. Click the list that is displayed beside the *Search* field to specify the search parameters. You can specify the following search parameters:

- *Search Title* This option allows you to search for a job by its name.
- *Search Keyword* This option allows you to search for a job by its keywords.
- *Search Description* This option allows you to search for a job by its description.
- *Search All Fields* This option allows you to search for a job by its title, keywords, and description.

3. Click the Search icon.

Related Information

To add an infoobject to a job [page 553]
To edit a job [page 552]

15.3.5 To edit a job

Context

This section describes how to edit a job.

> ⓘ Note
>
> - Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.
> - Editing a job does not amount to creating a new job.

To edit a job, complete the following steps:

1. Launch into the promotion management tool.
2. In the *Promotion Jobs* home page, select the job that you want to edit.
3. Click *Edit*.
   The details of the selected job are displayed. You can add or remove infoobjects, manage dependencies or promote the job, as necessary.

Results

While editing a job, you cannot change the name of the source system.

Related Information

To add an infoobject to a job [page 553]
To promote a job when repositories are connected [page 556]

To schedule a job promotion [page 563]

15.3.6 To add an infoobject to a job

Context

Each job must include a set of infoobjects. Hence, you must add infoobjects to a job before you promote it to the destination system.

> **Note**
>
> - When you promote a Crystal report based on Business View infoobjects (Data Connection, Data Foundation, Business Elements, and Business View) you must include the security information (DataAccess right on Data Connection and the ViewDataField right on Data Foundation and Business Elements) to see data in a report on the destination system.
> - Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To add an infoobject to a job, complete the following steps:

Procedure

1. Launch the promotion management tool.
2. Create a new job or edit an existing job.
   For information on creating a new job, see To create a job [page 548] and To edit a job [page 552].
3. Click *Add Objects* if editing a job.

   > **Note**
   >
   > The *Add Objects* dialog box is displayed when creating a new job..
4. Navigate to the folder from which you want to select the infoobject.
   The list of infoobjects in the selected folder is displayed.
5. Select the infoobject that you want to add to the job, and click *Add*

   If you want to add an infoobject and exit the "Add Objects from the System: `<NAME>`" dialog box, click *Add and Close*. The infoobject is appended to the job and the dialog box closes.

Results

After you add an infoobject to a job, you can right-click the *Job Viewer* page and select promotion processes to proceed with the promotion task. You can manage the dependents of the infoobject you selected using the *Manage Dependencies* option in the *Job Viewer* page.

> **Note**
>
> - The Shopping Cart, which is displayed in the left panel of the *Job Viewer* page, displays the job, along with its dependents, in a flat tree structure.
> - Click *Save* option after adding infoobjects, to save the changes. Otherwise, the user is prompted with an option to save the job when the user closes the tab.

Best Practice: SAP BusinessObjects recommends that you select a small number of infoobjects, which should not exceed 100 at a time, for promotion to obtain optimum performance of the promotion management tool.

Related Information

To manage the dependencies of a job [page 554]
To promote a job when repositories are connected [page 556]
To schedule a job promotion [page 563]

15.3.7 To manage the dependencies of a job

Context

This section describes how to manage the dependents of an infoobject.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To manage the dependents of an infoobject, complete the following steps:

Procedure

1. Launch the promotion management tool.
2. Create a new job or edit an existing job.
   For information on creating a new job, see To create a job [page 548] and To edit a job [page 552].
3. Add the required infoobjects to the job and close the *Add Objects* dialog to return to the *Job Viewer* window.
4. Click *Manage Dependencies*.
   The *Manage Dependencies* window is displayed. This window displays the list of infoobjects and their dependents. To view only the object dependents that have not been selected, click *Show unselected Dependents* check box.

5. From the *Select Dependents* drop-down list, select the options to add the grouped dependents to the job. The dependents are not selected by default; you must explicitly select the dependents you want to promote.

   For example, if you select *All Universes* from the *Select Dependents* drop-down list, then all universes included in the list of dependents are selected. You can also select the dependents individually.

   You can click the *Type* to view the supported filtering options for the infoobjects. A drop-down list is displayed. This list displays the supported filtering options. Select the filtering option, and click *OK*. The filtered infoobjects are displayed.

   When you select the dependents from the *Dependents* column, and click *Apply Changes* the dependents are automatically moved to the *Objects in Job* column.

   You can also type the name of the dependent in the *Search Dependents* field to search for a dependent.

   For more information on searching for dependents, see To search for dependents [page 555]
6. Click *Apply Changes* to update the list of dependents and click *Apply Changes and Close* to save the changes.

Results

Dependent objects are computed automatically by the tool. These dependents are computed based on either the infoobject relationships or infoobject properties. Dependents that do not qualify under either of these are not computed in this version of the tool.

> ⓘ Note
>
> If you select a folder for promotion, then the contents in the selected folder are considered as primary resources.

Related Information

To promote a job when repositories are connected [page 556]

15.3.8 To search for dependents

The advanced search feature in the promotion management tool allows you to locate the dependents of infoobjects that are available in the repository.

> ⓘ Note
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To search for the dependents of an infoobject, complete the following steps:

1. Launch promotion management.
2. Create a new job, or edit an existing job.
   If you have created a new job, add infoobjects to the job. If you are editing an existing job, you can add objects, as necessary.
3. Click *Managing Dependencies*.
4. In the *Search Dependents* field, enter the name of the dependent you want to locate.
5. Click the Search icon.

Related Information

To manage the dependencies of a job [page 554]

15.3.9 To promote a job when repositories are connected

Context

This section describes how to promote a job from the source system to the destination system if both systems are live.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

The following table lists the infoobject types that can be promoted using the promotion management tool:

Category	Object types you can promote
Reports	Crystal reports, Web Intelligence, QaaWS, Lumira
Third-Party Objects	Rich text, Text document, Microsoft Excel, Microsoft Power Point, Microsoft word, Flash, Adobe acrobat
Users	Users and user groups
Server	Server groups
Business Intelligence Platform	Folder, Program, Events, Profiles, Object package, HyperLink, Categories, Inbox document, Personal and Favorites folder
Universe	Universes and Connections
EPM Dashboard	Universes, Connections, Reports, and Analytics
BusinessView	DataFoundation

Category	Object types you can promote
Federation • Replication List • Replication Jobs	Replication List promotes the following objects: Flash, .txt, Discussions, .pdf, Hyperlink, .xls, ObjectPackage, Crystal Reports, Web Intelligence documents, Universes, Program, Connections, DataFoundation, Business Views, .rtf, Profile, Event, Users, and userGroups. Replication Connections promotes Replication Jobs, Remote Connection, Publications, Discussion, Pioneer Connection
BI Services	Web Intelligence Documents, Universes and Connections
New Infoobjects	Crystal reports (rpt/rptr), Pioneer, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Data Foundation (DFX), Webl, Data Federator, Data Steward, BI Workspace, etc.
Tenants	Promotion Management supports promotion of tenants, along with its dependencies, from source to the destination system by providing options to select and add tenants and corresponding tenant objects to a job. It also establishes a relationship between tenants and the corresponding tenant objects as dependencies. The feature works in both GUI and CLI mode of promotion management.

BI Commentary is supported in Promotion Management. When you promote a document with comments, any comments on the document are also migrated from source to destination system (Live to Live, Live to BIAR, BIAR to Live). To promote a document with comments, choose *Promote* > *Commentary Settings* and select the *Include Comments* checkbox .

> **Note**
>
> By default, the *Include Comments* checkbox is not selected.

When you promote a replicated objects , the replication-specific information associated with the objects also promoted from source to destination system (Live to Live, Live to BIAR, BIAR to Live). To promote a document without replication-specific information, choose *Promote* > *Federation Jobs Settings* and de-select the *Include Federation Jobs Relationship* checkbox.

> **Note**
>
> By default, the *Include Federation Jobs Relationship* checkbox is selected.

To promote a job, complete the following steps:

Procedure

1. Launch promotion management.
2. In the *Promotion Jobs* home page, select the job you want to promote.
   You can also right-click the home page screen, and click *Promote*.
3. From the *Destination* system list, select a different destination system as necessary.

   > **Note**
   >
   > Ensure that you have logged into both source and destination systems before you proceed with promotion process.

4. In the *Change Management ID* field, enter the appropriate value, and click *Save*.

> **Note**
>
> The Change Management ID is used for obtaining information related to logging, auditing, job history. The promotion management tool allows you to map each instance of job creation to a Change Management ID. The Change Management ID is an attribute that is set by the user in the job definition while creating a new job. The tool automatically generates an ID for each job.

5. Select *Security Settings*, as necessary. The following options are displayed:
   - *Do not promote security* This is the default option.
   - *Promote security* Use this option to promote jobs along with the associated security rights.
   - *Promote object security* Use this option to promote the security of objects and folders
   - *Promote user security* allows you to promote the rights of the users who are a part of the job
   - *Include Application Rights* You can select this option only when you also select *Promote User Security*. If the objects in the job inherit any application rights, the job is promoted along with those rights.
   - *Promote Top-Level Security* Use this option to promote the top level security rights.

     > **Caution**
     >
     > The *Promote Top-Level* security option overwrites the top level security rights defined in the target system.

   You can also click *View Rights* to view the security dependencies of infoobjects in the job.

> **Note**
>
> The *View Rights* button is disabled until you save the new job.

6. Click *Save*.

   The *View Rights* button is enabled. You can now view security dependencies.
7. Click *Test Promote* to ensure that there are no conflicts between CUIDs of infoobjects in the source and destination systems. The promotion details are displayed under the tabs *Success*, *Failure* and *Warning*. The first column displays the objects to be promoted, and the second column displays promotion status of each infoobject. The promotion management tool classifies the selected objects into users, groups, universes.

> **Note**
>
> This option does not commit any infoobjects for promotion.

   The result of a test promote can be any one of the following:
   - `Overwritten` The infoobject in the destination system is overwritten by the infoobject in the source system.
   - `Copied` The infoobject in the source system is copied to the destination system.
   - `Dropped` The infoobject is not promoted from the source system to the destination system.
   - `Warning` The infoobject in the destination system is the newer version and you can remove the infoobject from the Job. However, if you want to promote, the infoobject gets promoted.
   - `Mapped` The infoobject is mapped to an infoobject on the destination system.
8. Click *Schedule* if you want promotion to run at a specific time or on a recurring schedule.

9. Click *Promote*.
   The selected job is promoted.

Results

If you do not want to promote the job, you can use the *Save* option to save the modifications such as Security, Change Management ID, and Schedule settings.

15.3.10 Promoting a job using an LCMBIAR File

Promoting refers to the activity of transferring a BI resource from one repository to another. If the source system and destination system are on the same network, the promotion management tool uses WAN or LAN to promote the infoobject. However, the promotion management tool also facilitates the promotion of infoobjects even if the source and destination systems are not on the same network.

In scenarios where the source and destination systems are not on the same network, the promotion management tool supports the promotion of jobs to the destination system by enabling you to export the job in the source system to an LCMBIAR file and import the job from the BIAR file to the destination system.

This section describes how to export a job to an LCMBIAR file and then import the job from the BIAR file to the destination system.

> ⓘ Note
>
> - Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.
> - Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

Related Information

Exporting a job to an LCMBIAR File [page 559]
Importing a job from an LCMBIAR File [page 560]

15.3.10.1 Exporting a job to an LCMBIAR File

Context

This section describes how to export a job to an LCMBIAR file.

To export a job to an LCMBIAR file, complete the following steps:

Procedure

1. Launch the promotion management tool, and create a new job.
   For more information on creating a new job, see To create a job [page 548]
2. From the *Destination* drop-down list, select *Output to LCMBIAR file* option and click *Create*.
3. Click *Add Objects* to add infoobjects to the job.

   You can use the *Manage Dependencies* option to manage the dependencies of the selected job.
4. To encrypt the LCMBIAR file using password, click *Password Encryption* checkbox.
5. Enter a password in the *Password* field.
6. Re-enter the password in the *Verify Password* field.
7. Click *Promote*.
   The *Promote* window is displayed.
8. Modify the security options as needed and click *Export*.
   The LCMBIAR file is created. You can save the LCMBIAR file to the file system.
9. (Optional) Click *LCMBiar File Destination* and select *FTP* or *SFTP* to export the LCMBIAR file to an FTP server or an SFTP server respectively. Enter the hostname, port, username, password, directory, and filename and click *Export*.

   > **Note**
   >
   > If you choose *SFTP* as the *LCMBiar File Destination*, you need to additionally enter the SFTP fingerprint.
10. From the *Destination* drop-down list, select *Output to LCMBIAR file*, and click *LCMBIAR File Destination*.

Results

You can schedule the export of a job to an LCMBIAR file. For more information on this, refer to the To schedule a job promotion [page 563] section.

Related Information

To add an infoobject to a job [page 553]
To manage the dependencies of a job [page 554]

15.3.10.2 Importing a job from an LCMBIAR File

Prerequisites

You can import a job from an LCMBIAR file. The LCMBIAR file is copied from the storage device to the destination system.

Context

To import an LCMBIAR file, complete the following steps:

Procedure

1. Launch the promotion management tool.
2. In the *Promotion Jobs* home page, click *Import* > *Import file*.
   The *Import from file* window is displayed.
3. You can import a BIAR file from the file system or from an FTP or an SFTP server.
   - To import a BIAR file from the file system, perform the following steps :
     1. Select *file system*.
     2. Click *Browse* and select an LCMBIAR file from the file system.
     3. In the *Password* field, enter the password of the LCMBIAR file.

        > **Note**
        >
        > The Password field is displayed only if the LCMBIAR file is encrypted with a password.

     4. Click *Create*. The job is created.

        > **Note**
        >
        > If a job with the same name exists, the Confirm Save popup is displayed. Click 'Yes' to overwrite the existing job; Click 'No' to create a job with a new name `jobname_copy<CURRENT_DATE_AND_TIME>`
   - To import an LCMBIAR file from an FTP server, complete the following steps:
     1. Select *FTP*.
     2. Enter appropriate details in the host, port, username, password, directory, and filename fields and click *OK*.
   - To import an LCMBIAR file from an SFTP server, complete the following steps:
     1. Select *SFTP*.
     2. Enter appropriate details in the host, port, username, password, directory, fingerprint, and filename fields and click *OK*.
4. Click *Promote*.
   The *Promote - Job Name* window is displayed.
5. From the *Destination* drop-down list, select the destination system. If you select *Login to a New CMS*, you will be prompted for credentials. Confirm the login credentials of the destination system.
6. Click *Promote* to promote the contents to the destination system.

   You can also click the *Test Promote* option to view the objects to be promoted and the promotion status.
7. **Optional:** If you're importing a Web Intelligence document that uses customization, in the *User Groups BI Preferences* tab, make sure to check *Overwrite User Groups BI Preferences* to import the customization.

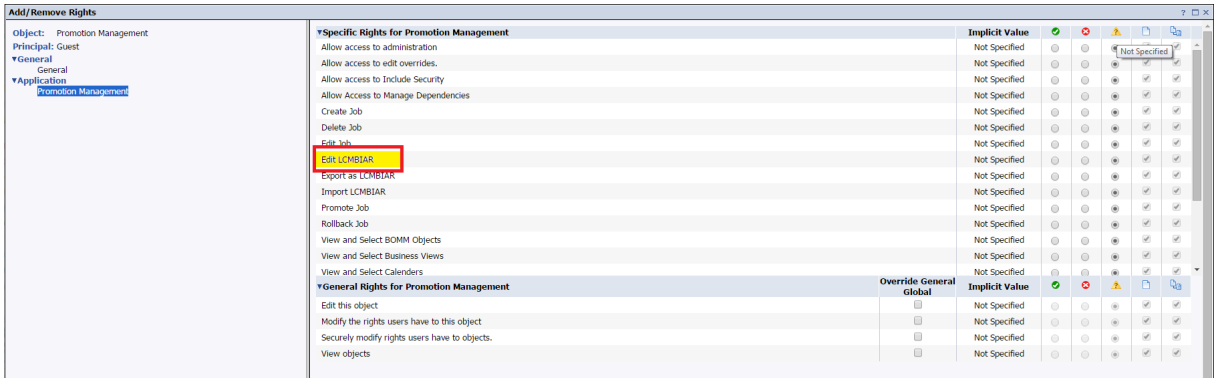
Related Information

To manage the dependencies of a job [page 554]

15.3.10.2.1 Selective retrieval of objects from an LCMBIAR file

Prerequisites

To selectively retrieve objects from an LCMBIAR file, it is required that the user have *Edit LCMBIAR* right.



Context

To selectively retrieve objects from an LCMBIAR file, perform the following:

Procedure

1. Select the objects to be promoted.
2. Click *Promote*.

> **Note**
>
> - A new job with the selected objects is created.
> - The same operation can be performed using the Command line tool. For more information, see Command Line tool parameters [page 577]
> - Selective promotion is not supported for live to live scenario.

15.3.11 To schedule a job promotion

Context

This section describes how to schedule the promotion of a job. It also describes how to specify the recurrence options and parameters.

> ⓘ Note
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To schedule the promotion of a job instance, complete the following steps:

Procedure

1. In the *Promote* dialog box, click the *Schedule* option.
2. Set the required schedule option and click *Schedule*.

Results

If you add InfoObjects to a folder contained in a job after the job has been scheduled for promotion, they will also be promoted to the destination at the scheduled time. However, this does not hold true when you try to schedule a job promotion using an LCMBIAR file, as LCMBIAR is not considered as a 'real' destination.

> → Tip
>
> After the promotion of a job is complete, you can view all instances of the job by selecting the job on the *Promotion Jobs* page and clicking *History* on the toolbar.

Promotion of a job can also happen based on event triggers.

You can select email notifications based on job promotion status (like success/partial success/failed).
For detailed information on the various scheduling options and configuring your notifications, refer to the Scheduling section.

Related Information

Exporting a job to an LCMBIAR File [page 559]

15.3.11.1 To update the recurring and pending job promotion instances

Context

The promotion management tool allows you to track the status of and reschedule promotion job instances using the *Recurring and Pending Instances* option.

To track the statys of and reschedule promotion job instances, complete the following steps:

Procedure

1. Launch the promotion management tool.
2. In the *Promotion Jobs* home page, select a job.
3. Click *History*.
   The *Job History* window is displayed.
4. Click *Recurring & Pending Instances*.
   The *Job History for Recurring and Pending Instances* window is displayed. This window displays the list of recurring and pending promotion job instances.

   You can use the following options, as necessary:
   - Click *Promoted Instances* to view the list of promoted job instances.
   - Click the *Pause* option to pause the selected pending or recurring instance.
   - Click the *Resume* option to resume the paused scheduled promotion job instance.
   - Click the *Reschedule* option to reschedule the selected promotion job instance.
   - Click to delete a scheduled promotion job instance.
   - Click to refresh the status of a scheduled promotion job instance.
   - You can use the option to navigate a single page, or navigate to a specific page by entering the relevant page number.

   > **Note**
   >
   > The status column in the *Job History for Recurring and Pending Instances* window displays the status of the promotion job instance, such as recurring, pending.

Related Information

To roll back a job [page 565]

15.3.12 To view the history of a job

Context

This section describes how to view the history of a job.

> **Note**
>
> To view the history of a job, you must ensure that the status of the job is one of the following:
>
> - Success
> - Failure
> - Partial Success

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To view the history of a job, complete the following steps:

Procedure

1. Launch the promotion management tool.
   The *Promotion Jobs* home page is displayed.
2. Select the job for which you want to view the history, and click the *History* tab.

   The job instance time, name of the job, names of the source and destination systems, the ID of the user who promoted the job, and the status (Success, Failure, or Partial Success) of the job are displayed.

   You can view the detailed status of the job by using the link displayed in the *Status* column.

15.3.13 To roll back a job

Context

The Rollback option allows you to restore the destination system to its previous state, after a job is promoted.

> **Note**
>
> Security enhancements is implemented in the promotion management tool, resulting in changes to certain behaviors when executing actions. For more information, please refer 3350454.

To roll back a job, complete the following steps:

Procedure

1. Launch the promotion management tool.
   The *Promotion Jobs* home page is displayed.
2. Perform any of the following operations:
   - Right-click the job you want to roll back, and select *Rollback*.
   - Select the job you want to roll back, and click the *Rollback* tab.

   The *Rollback* window is displayed.
3. Select the instance you want to roll back, and click *Complete Rollback*.
   The instance is rolled back.

Results

You can roll back only the most recent instance of a promotion job. You cannot roll back multiple job instances simultaneously.

15.3.13.1 To use the Partial Rollback option

Context

The promotion management tool allows you to roll back infoobjects in a job either completely or partially from the destination system.

To roll back infoobjects partially, complete the following steps:

Procedure

1. Launch the promotion management tool.
   The *Promotion Jobs* home page is displayed.
2. Perform any of the following operations:
   - Right-click the job you want to rollback, and select *Rollback*.
   - Select the job you want to rollback, and click the *Rollback* tab.

   The *Rollback* window is displayed.
3. Select the instance from the list, and click *Partial Rollback*.

   The list of infoobjects in the selected job is displayed in the *Job Viewer* page.
4. Select the infoobjects that you want to roll back, and click *Rollback*.

Next Steps

> **Note**
>
> You must ensure that you have rolled back all the infoobjects in an instance before you roll back infoobjects in the next instance.

> **Caution**
>
> If a job is promoted with security, then, during the partial rollback of infoobjects, the selected dependent infoobjects may not have their security rolled back to their previous states.

Related Information

To manage different versions of BI resources [page 618]

15.3.13.2 To roll back a job after the password expires

This section describes how to roll back a job, after the password that was used to promote it expires.

To roll back a job after the password expires, complete the following steps:

1. Select the job that you want to roll back, and click *Rollback*.
2. In the *Rollback* window, select *Complete Rollback*.
   An error message is displayed. This message states that the job cannot be rolled back. You are also prompted to log into the source or destination system.
3. Enter the new login credentials, and click *Login*.

A dialog box is displayed indicating that the rollback process is complete.

> **Note**
>
> The jobs that were promoted using the source or destination system credentials are updated automatically.

Related Information

To partially roll back infoobjects after the password expires [page 568]
To use the Partial Rollback option [page 566]

15.3.13.2.1 To partially roll back infoobjects after the password expires

This section describes how to partially roll back infoobjects, after the password for the source or destination system expires.

To partially roll back infoobjects after the password expires, complete the following steps:

1. Select the job that you want to roll back, and click *Rollback*.
   The *Rollback* window is displayed.
2. Select the *Partial Rollback* option.
   An error message is displayed. This message states that the infoobjects cannot be rolled back. You are also prompted to log into the source or destination system.
3. Enter the new login credentials, and click *Login*.
   The *Job Viewer* page is displayed. This page displays the list of infoobjects.
4. Select the required infoobjects, and click *Rollback*.

> **Note**
>
> The jobs that were promoted using the source or destination system credentials are updated automatically.

Related Information

To roll back a job [page 565]
To use the Partial Rollback option [page 566]
To roll back a job after the password expires [page 567]

15.4 Promoting full repository content using the promotion management tool

Promoting the contents of a repository requires planning, preparation, and sufficient time. This section describes the actions required for a successful promotion of content from one deployment to another.

15.4.1 To prepare the source and target systems

Context

You must ensure that the source and target systems are configured optimally before promoting content.

Procedure

1. On the source system:
   a. Use the Repository Diagnostic Tool (RDT) to scan and fix the source system and correct any repository or FRS inconsistencies. For more information on the RDT, see the *Business Intelligence Platform Repository Diagnostic Tool User Guide*.
   b. Minimize system usage on the source system to ensure minimal changes during promotion. An active system can result in object failure.

      > **Note**
      >
      > If failures occur, review the job status to rectify any issues.

2. On the target system:
   a. Use the license keycode to ensure that the correct and sufficient license is set on the target system.

      > **Note**
      >
      > To avoid content promotion failure due to insufficient licensing, use identical licensing on both systems.

   b. If you use third-party authentication, you must configure and enable it on the target system prior to promoting content.

      > **Note**
      >
      > Do not map users or user groups. This will result in the creation of users or user groups with different CUIDs on the target system. The promotion process uses CUIDs to identify and map objects between the source and target system. Mapping users and user groups will cause content mismatches and will result in promotion failure.

   c. Ensure that all required add-ons on the source system are also installed on the target system.

      > **Note**
      >
      > To ensure successful migration, you must install add-ons such as Analysis or Design Studio on the source system.

   d. If you have content that uses QaaWS connections, you must enable the overrides to ensure that these connections point to the correct web services. For more information on setting up overrides, see the "Overrides" section.
   e. If you need to migrate all completed scheduled instances, you must click *Show completed instances in Manage Dependencies page* in the *Job Settings* of Promotion Management.
3. On the central system:
   a. You can designate the source system, the target system, or a separate system as the central system, where the Promotion Management jobs are executed. When promoting a full repository, you will handle a large amount of content that will require additional system resources on the central system. Use the following sizing reference to configure the central system for 10,000 objects:

	Temporary Space Allocation	Memory Allocation	Additional Configuration
`LCM_CLI`	2 GB	2 GB	Update `LCM_CLI.bat` and change the `-Xmx` parameter.
Promotion Management Job Server	3 GB	3 GB	In the CMC, update the Promotion Management Job Server start-up property by adding the `-javaargs Xmx3g` parameter. For more information, please refer to SAP Note 2286419.

For example, if you estimate the job to contain 50,000 objects:

- Allocate 10 GB of memory to `LCM_CLI` (50,000 ÷ 10,000 × 2)
- Allocate 15 GB of memory to the Job Server (50,000 ÷ 10,000 × 3)

> **Note**
>
> These sizing guidelines apply to most environments. However, the size of documents may affect resource requirements.

15.4.2 Migration strategies

- Use the Command-Line Interface (CLI) rather than the web CMC tool for all job promotions.
  - The CLI bypasses the twenty-minute web session limit which is involved during a promotion job that includes more than 1,000 objects.

    > **Note**
    >
    > The object limit depends on sufficient system resources.

  - The CLI provides granular control over content promotion by using query language to select the content to be migrated. You can select content of the same type or content located in the same directory.
  - The CLI can be run in batches and promotion jobs can be initiated by other scripting tools.
- Establish security by promoting the principals (users and user groups) first.
  - Promoting the users and user groups first preserves the security model on the target system and ensures the success of subsequent migration of the users' personal content (such as inboxes, favorites, and personal categories).

    > **Note**
    >
    > It is important that you perform this task first so that the CUIDs of the users and user groups on the target system will be identical to those on the source system.

- Turn off dependency calculation.
  - Dependency calculation is one of the most intensive tasks in the job creation process. During full repository migration, all objects are migrated, making the calculation unnecessary.

    > ⓘ Note
    >
    > This feature is useful only when you are unsure of which dependent objects are required.

- Avoid including security calculation whenever possible.
  - Security calculation is the second-most intensive task in the job creation process. Break up the promotion into two jobs if you have many documents in different directories, and security is set only on the directories. The first job should contain only objects with security enabled and the second job should contain only documents with security disabled. In this manner, you can perform security calcuations only on the directories, avoiding calculating security on all documents.

    > ⓘ Note
    >
    > Object security is preserved because it is inherited from folder security.

15.5 Full system promotion steps

A full system promotion requires the execution of three separate promotion jobs in order, each promoting specific content types. For more information on how to promote multiple objects, refer to Knowledge Base Article 1969259.

The following table outlines the content types and parameter settings for each promotion job.

Promotion Job	Content Type	`exportDependencies`	`includeSecurity`
1	All users and user groups	false	true
2	All dependent objects	false	true
3	All primary objects	false	true

Use the Command-Line Interface (CLI) to create and execute each job. For more information on the CLI, see the Using the Command Line option [page 575] section.

Common Parameters

USe the following parameters for all three promotion jobs:

> → Remember
>
> Ensure that each parameter is on a new line.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
```

```
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

15.5.1 To promote users and user groups (Job 1)

Context

To establish identical security models between the source and target systems and to ensure that the user and user groups objects' CUIDs are identical, promote the users and user groups first.

Procedure

1. Create a the `usersandgroups.properties` file with the common parameters and append the following parameters to the file in order to select all users and user groups:

   ```
   exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
   SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
   (SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2,
   3))
   ```

2. To execute the job, navigate to `<INSTALLDIR>\win64x64\scripts` directory and run the following command:

   ```
   Lcm_cli.bat –lcmproperties=usersandgroups.properties
   ```

15.5.2 To promote dependent objects (Job 2)

Context

Dependent objects are depended upon by the primary objects in the Public folder and the users' Favorites folder. To eliminate the need to set `includeDependencies` to `true` for all other jobs, promote the dependent objects second. The following are dependent objects:

- Access Levels
- Applications
- BusinessViews

- Calendars
- Categories
- Connections
- Events
- OLAP Connections
- Profiles
- Projects
- QaaWS
- Remote connections
- Replication lists
- Server Groups
- Universes

Procedure

1. Create the dependencies.properties file with the common parameters and append the following parameters to the file in order to select all dependent objects:

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target
and set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and
si_specific_kind != 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
```

```
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID =
'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. To execute the job, navigate to `<INSTALLDIR>\win64x64\scripts` directory and run the following command:

```
Lcm_cli.bat –lcmproperties=dependencies.properties
```

15.5.3 To promote primary objects (Job 3)

Context

Primary objects are core BI documents that reside in the Public folder and the users' Favorites folder. Assuming that the second promotion job has already been executed, migrating all the dependent objects, promoting primary objects last re-establishes their relationships with dependent objects.

Procedure

1. Create a the `primaryobjects.properties` file with the common parameters and append the following parameters to the file in order to select all users and user groups:

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

   If you re-run the same job, exclude the LCM job using the following query:

```
SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
```

```
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") and SI_KIND not in
('LCMJob')
```

2. To execute the job, navigate to `<INSTALLDIR>\win64x64\scripts` directory and run the following command:

```
Lcm_cli.bat –lcmproperties=primaryobjects.properties
```

> **Note**
>
> If there are more than 50,000 objects in the Public folder or the users' Favorites folders, it may be necessary to break this final job into smaller jobs.

> **Note**
>
> Ensure that the machines running the Command-Line interface command and the Promotion Management Job Server both meet the sizing requirements. For more information, see the “Sizing” section.

15.5.4 Post-promotion

Promotion Management promotes only the server groups, but not their servers. To ensure that reports with designated servers will continue to work, you must recreate and assign the servers to the correct server groups.

15.6 Using the Command Line option

The command line option of the promotion management tool allows promoting objects from one BI platform deployment to another. You can create a batch script for multiple jobs.

> **→ Tip**
>
> Use the command line option for jobs that contain a large number of objects.

The promotion management tool supports the following job promotion types from the command line:

- Export an existing promotion job template to LCMBIAR with password encryption
- Export an existing promotion job template to LCMBIAR without password encryption
- Export single or multiple platform queries
- Promote multiple platform queries
- Promote with an existing job template
- Import and promote an existing LCMBIAR file
- Perform Live-to-Live promotion

15.6.1 To run the command-line tool on Windows

Context

To run the command line tool, complete the following steps:

Procedure

1. Launch a command line window or shell.
2. Navigate to the appropriate directory.

   For example, the directory path for windows is -`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Do one of the following:
   - Execute the LCMCLI, ensure the java path is set prior to running the program.
     Command: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <property file>`
   - Run the BAT file from `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat`
     Command: `lcm_cli.bat -lcmproperty <property file>`

     > **Note**
     >
     > Enter the valid passwords when prompted.

Results

The promotion management command line tool takes a `<properties>` file as a parameter. The `<properties>` file contains the required parameters to communicate with the promotion management tool about the actions to perform, connection to which BI platform deployment, connection methods, objects to promote.

The file must be in the form of `<FILENAME>.properties`

For Example: `<Myproperties.properties>`

15.6.2 To run the command-line tool on Unix

Context

To run the command line tool, complete the following steps:

Procedure

1. Launch shell.
2. Navigate to the appropriate directory.
   For example, `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib`
3. Do one of the following:
   - Execute the LCMCLI, ensure the java path is set prior to running the program.
     Command: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <property file>`
   - Run the BAT file from `<installdir_path>\sap_bobj\lcm_cli.sh`
     Command: `lcm_cli.sh -lcmproperty <property file>`

> ⓘ Note
>
> Enter the valid passwords when prompted.

15.6.3 Command-line tool parameters

The command-line parameters for the command-line option of the promotion management tool are organized according to three main promotion types:

- Promoting objects from a LCMBIAR file to a live CMS
- Promoting objects from a source live CMS to a target live CMS
- Exporting objects from a live CMS to a LCMBIAR file

In addition to the parameters concerned by these three promotion types, there are also parameters for general commands which can be used in all promoting scenarios.

> → Remember
>
> Do not place command-line parameters within quotation marks.

> ⓘ Note
>
> - Similar to the creation of a job before exporting, the Command Line option creates a temporary job on the fly. This job name could be a combination of `Query_<USER>_<Timestamp>`. This is specific only to `<exportQuery>`.
> - You can rollback the job only through the promotion management tool. There is no command line support to rollback the jobs.
> - When working with a large number of objects, it is recommended to increase the maximum Java heap size by setting the `-Xmx=8g` parameter in the `LCMCLI` script.

Related Information

LCMBIAR file to a live CMS [page 581]
Source live CMS to a target live CMS [page 587]
Live CMS to a LCMBIAR file [page 584]
List of all the command line parameters [page 591]

15.6.3.1 Command line parameters by promotion scenario

The command line parameters are presented in the recommended order for each promotion scenario. The table indicates all of the available parameters and their status as mandatory or optional for each promotion scenario. Each mandatory parameter is described for its corresponding promotion scenario. The optional parameters are described in the List of all the command line parameters section. Refer to Related Links for all parameter information by scenario and the available additional parameters.

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
Properties file	`lcmproperty`	Optional	Recommended	Recommended	Recommended
Action type	`action`	Mandatory action=promote	Mandatory action=export	Mandatory action=promote	Mandatory action=rollback
LCM Node	`LCM_CMS`	Mandatory			
	`LCM_userName`	Mandatory			
	`LCM_Password`	Mandatory If empty, it will be required in the console			
	`LCM_authentication`	Optional: Default = `secEnterprise`			
	`LCM_SystemID`	Mandatory only for SAP authentication			
	`LCM_ClientID`	Mandatory only for SAP authentication			
Source (live or LCMBIAR)	`importLocation`	Mandatory	Not Applicable	Not Applicable	Not Applicable
	`lcmbiarpassword`	Mandatory (can be empty)	Not Applicable	Not Applicable	Not Applicable

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
	`Source_CMS`	Not Applicable	Mandatory	Mandatory	Not Applicable
	`Source_UserName`	Not Applicable	Mandatory	Mandatory	Not Applicable
	`Source_password`	Not Applicable	Mandatory If empty, it will be required in the console	Mandatory If empty, it will be required in the console	Not Applicable
	`Source_authentication`	Not Applicable	Optional Default = `secEnterprise`	Optional Default = `secEnterprise`	Not Applicable
	`Source_systemID`	Not Applicable	Mandatory only for SAP authentication	Mandatory only for SAP authentication	Not Applicable
	`Source_clientID`	Not Applicable	Mandatory only for SAP authentication	Mandatory only for SAP authentication	Not Applicable
Destination (Live or LCMBIAR)	`Destination_CMS`	Mandatory	Not Applicable	Mandatory	Not Applicable
	`Destination_username`	Mandatory	Not Applicable	Mandatory	Not Applicable
	`Destination_password`	Mandatory	Not Applicable	Mandatory	Not Applicable
	`Destination_authentication`	Optional Default = `secEnterprise`	Not Applicable	Optional Default = `secEnterprise`	Not Applicable
	`Destination_systemID`	Mandatory only for SAP authentication	Not Applicable	Mandatory only for SAP authentication	Not Applicable
	`Destination_clientID`	Mandatory only for SAP authentication	Not Applicable	Mandatory only for SAP authentication	Not Applicable
	`ExportLocation`	Not Applicable	Mandatory	Not Applicable	Not Applicable
	`lcmbiarpassword`	Not Applicable	Mandatory (can be empty)	Not Applicable	Not Applicable
Job related	`JOB_CUID`	Not Applicable	Optional	Optional	Mandatory

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
	`Override`	Optional	Not Applicable	Not Applicable	Not Applicable
	`forceOverride` Available in SP4	Optional	Not Applicable	Not Applicable	Not Applicable
	`Timeout` Available in SP4	Optional	Not Applicable	Optional	Not Applicable
Export related	`ExportDependencies`	Not Applicable	Optional Default = `False`	Optional Default = `False`	Not Applicable
	`ExportQuery`	Not Applicable	Mandatory	Mandatory	Not Applicable
	`ExportQueriesTotal`	Not Applicable	Optional: Use when you have more than one export query	Optional: Use when you have more than one export query	Not Applicable
	`BatchJobQuery`	Not Applicable	Optional: Use with Exportquery	Optional: Use with Exportquery	Not Applicable
	`LimitQueryBatchSize`	Not Applicable	Optional	Optional	Not Applicable
Log related	`Consolelog`	Optional Default = `False`	Optional Default = `False`	Optional Default = `False`	Not Applicable
	`ResultFileName`	Optional	Optional	Optional	Not Applicable
	`LogFileName` Available in SP4	Optional	Optional	Optional	Not Applicable
Object selection	`Selected_CUIDS`	Optional	Not Applicable	Not Applicable	Not Applicable
	`selectUser` Available in SP4	Not Applicable	Optional Default=`All`	Optional Default=`All`	Not Applicable
	`selectGroup` Available in SP4	Not Applicable	Optional Default=`All`	Optional Default=`All`	Not Applicable
Security	`IncludeApplicationSecurity`	Optional Default = `False`	Optional Default = `False`	Optional Default = `False`	Not Applicable

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
	`IncludeSecurity`	Optional Default = `False`	Optional Default = `False`	Optional Default = `False`	Not Applicable
	`IncludeTopLevelSecurity`	Optional Default = `False`	Optional Default = `False`	Optional Default = `False`	Not Applicable
Comments	`IncludeComments`	Optional Default = `False`	Optional Default = `False`	Optional Default = `False`	Not Applicable
Federation Jobs	`IncludeFederationJobsRelationship`	Optional Default = `True`	Not Applicable	Optional Default = `True`	Not Applicable

Related Information

LCMBIAR file to a live CMS [page 581]
Live CMS to a LCMBIAR file [page 584]
Source live CMS to a target live CMS [page 587]
List of all the command line parameters [page 591]

15.6.3.2 LCMBIAR file to a live CMS

When you are promoting objects from an LCMBIAR file to a live CMS you reference a properties file from the command line that specifies the promotion order as follows:

- Import location and the promotion action type.
- Login credentials to the CMS hosting the promotion management tool (previously called the lifecycle management tool LCM).
- Login credentials for the destination CMS.
- Other parameters required to successfully promote the CMS, for example the LCMBIAR password, or over ride setting to write over existing objects when required.

You can include other optional parameters that can specify particular promotion needs. These optional parameters are described in the section List of all the command line parameters [page 591].

The following example shows a case for a promotion LCMBIAR file to live CMS without using a property file in the Command line:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
```

```
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\Samples\webi\WebISamples.lcmbiar" -
lcmbiarpassword
```

The following example shows a case for a promotion LCMBIAR file to live CMS with a property file in the Command line:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
LCM command line property file
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:\Backup\CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

The following table lists the mandatory parameters required for a successful properties file for a promotion LCMBIAR file to live CMS:

Parameter group	Parameter	Description
Action type	`action`	Operation that the CLI must perform. Value: export Example: `action=export`
LCM Node	`LCM_CMS`	CMS for the promotion management tool. Value: Free form text Example: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Account user name that the tool must use to connect to the promotion management tool CMS. Value: Free form text Example: `LCM_userName=adminLCM`

Parameter group	Parameter	Description
	`LCM_password`	Password of the user account. Value: Free form text Example: `LCM_password=my_adminpassword1`
Source: LCMBIAR file	`importLocation`	Location of the LCMBIAR file that contains the objects to be promoted. Value: Free form text. Must have `<.lcmbiar>` extension Example: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Enables the encryption and decryption of BIAR files using a password . Value: Free form text Example: `lcmbiar=validlcmbiarpassword`
Destination: Live CMS	`Destination_CMS`	CMS to which the tool must connect. Value: Valid CMS name Example: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	User account that the tool must use to connect to the BI Platform CMS. Value: Valid user name Example: `Destination_username=adminLCM`
	`Destination_password`	Associated password of the user account. Value: Valid password Example: `Destination_password=my_adminpassword1`

Related Information

Live CMS to a LCMBIAR file [page 584]
Source live CMS to a target live CMS [page 587]
List of all the command line parameters [page 591]

15.6.3.3 Live CMS to a LCMBIAR file

When you are promoting objects from a live CMS to a LCMBIAR file, you reference a properties file from the command line that specifies the promotion order as follows:

- Promotion action type: export
- Login credentials to the CMS hosting the promotion management tool (previously called the lifecycle management tool LCM).
- Login credentials for the source CMS.
- Destination directory for the LCMBIAR file.
- Other parameters required to successfully promote the CMS, for example the LCMBIAR password, or security settings.

You can include other optional parameters that can specify particular promotion needs. These optional parameters are described in the section List of all the command line parameters [page 591].

The following example shows a typical properties file for a promotion live CMS to LCMBIAR file:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
#
exportLocation=E:\LCMTEST\
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM
CI_INFOOBJECTS, CI_APPOBJECTS, CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID in (23)")
#
#When applicable...
#
exportDependencies=true
includeSecurity=true
#
#Options
```

```
#
consolelog=true
```

The following table lists the mandatory parameters required for a successful properties file for a promotion LCMBIAR file to live CMS:

Parameter group	Parameter	Description
Action type	`action`	Operation that the CLI must perform. Value: export Example: `action=export`
LCM Node	`LCM_CMS`	CMS for the promotion management tool. Value: Free form text Example: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Account user name that the tool must use to connect to the promotion management tool CMS. Value: Free form text Example: `LCM_userName=adminLCM`
	`LCM_password`	Password of the user account. Value: Free form text Example: `LCM_password=my_adminpassword1`
Source: Live CMS	`Source_CMS`	CMS to which the promotion management tool must connect. Value: Free form text Example: `Source_CMS=myCMS.mydomain.sap:6400`

Parameter group	Parameter	Description
	`Source_userName`	User account that the promotion management tool must use to connect to the BI platform CMS. Value: Free form text Example: `Source_username=adminLCM`
	`Source_password`	Password of the user account. Value: Free form text Example: `Source_password=my_adminpassword1`
Destination: LCMBIAR file	`exportLocation`	Specifies the location to place the LCMBIAR file after the objects have been exported and packaged. Value: Free form text. Must have `<.lcmbiar>` extension Example: `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Enables the encryption and decryption of BIAR files using a password . Value: Free form text Example: `lcmbiarpassword=validlcmbiarpassword`

Parameter group	Parameter	Description
Export related	`exportQuery`	Queries the source CMS to get the required objects for export to the LCMBIAR file. Value: Free form text. Use the CMS query language format. Example: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Note** You can have any number of queries in one properties file, but they must be named as exportQuery1, exportQuery2.

Related Information

LCMBIAR file to a live CMS [page 581]
Source live CMS to a target live CMS [page 587]
List of all the command line parameters [page 591]

15.6.3.4 Source live CMS to a target live CMS

When you are promoting objects from a source live CMS to a target live CMS, you reference a properties file from the command line that specifies the promotion order as follows:

- Promotion action type: Promotion
- Login credentials to the CMS hosting the promotion management tool (previously called the lifecycle management tool LCM).
- Login credentials for the source CMS.
- Login credentials for the destination CMS.
- Other parameters required to successfully promote the CMS, for example security or dependencies parameters.

You can include other optional parameters that can specify particular promotion needs. These optional parameters are described in the section List of all the command line parameters [page 591].

The following example shows a typical properties file for a promotion source CMS to target CMS:

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

The following table lists the mandatory parameters required for a successful properties file for a promotion source CMS to a target CMS:

Parameter group	Parameter	Description
Action type	`action`	Operation that the command line must perform. Value: Promote Example: `action=promote`
LCM Node	`LCM_CMS`	CMS for the promotion management tool. Value: Free form text Example: `LCM_CMS=myCMS.mydomain.sap:6400`

Parameter group	Parameter	Description
	`LCM_userName`	Account user name that the tool must use to connect to the promotion management tool CMS. Value: Free form text Example: `LCM_userName=adminLCM`
	`LCM_password`	Password of the user account. Value: Free form text Example: `LCM_password=my_adminpassword1`
Source: Live CMS	`source_CMS`	CMS to which the promotion management tool must connect. Value: Free form text Example: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_username`	User account that the promotion management tool must use to connect to the BI platform CMS. Value: Free form text Example: `Source_username=adminLCM`
	`Source_password`	Password of the user account. Value: Free form text Example: `Source_password=my_adminpassword1`
Destination: Live CMS	`Destination_CMS`	CMS to which the tool must connect. Value: Free form text Example: `Destination_CMS=myCMS1:myCMS2`

Parameter group	Parameter	Description
	`Destination_username`	User account that the tool must use to connect to the BI Platform CMS. Value: Free form text Example: `Destination_username=admin LCM`
	`Destination_password`	Associated password of the user account. Value: Free form text Example: `Destination_password=my_adminpassword1`
Export related	`exportQuery`	Queries the LCM tool executes to get the required objects for export to the target CMS. Value: Free form text. Use the CMS query language format. Example: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Note** You can have any number of queries in one properties file, but they must be named as exportQuery1, exportQuery2.

Related Information

LCMBIAR file to a live CMS [page 581]
Live CMS to a LCMBIAR file [page 584]
List of all the command line parameters [page 591]

15.6.3.5 List of all the command line parameters

The following table describes all the command line parameters.

> **Note**
>
> When running within a command line, parameters have this syntax `-<parameterName><space><parameterValue>`. Within a property file, parameters have this syntax `<parameterName>=<parameterValue>`.

Parameter group	Parameter	Description
Properties file	`lcmproperty`	Refers to the values required for the execution of a command, which are saved in a file. Value: The full path of the location where property file has been saved Example: `-lcmproperty C:\MyPropertyFile.properties`
Action type	`action`	Operation that the CLI must perform. Value: Promote or export Example: `action=promote`
LCM Node	`LCM_CMS`	CMS for the promotion management tool. Value: Free form text Example: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Account username that the tool must use to connect to the promotion management tool CMS. Value: Free form text Example: `LCM_userName=adminLCM`
	`LCM_Password`	Password of the user account. If empty, it will be required in the console. Value: Free form text Example: `LCM_password=my_adminpassword1`
	`LCM_authentication`	Indicates the authentication type to be used. Value: secEnterprise, secWinAD, secLDAP,secSAPR3. If not specified, `secEnterprise` is used. Example: `LCM_authentication=secEnterprise`

Parameter group	Parameter	Description
	`LCM_systemID`	Required for SAP authentication only. Value: System ID Example: `LCM_systemID=systemID`
	`LCM_clientID`	Required for SAP authentication only. Value: Client ID Example: `LCM_clientID=clientID`
Source: LCMBIAR file	`importLocation`	Location of the LCMBIAR file that contains the objects to be promoted. Value: Free form text. Must have `<.lcmbiar>` extension Example: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Enables the encryption and decryption of BIAR files using a password . Value: Free form text Example: `lcmbiar=validlcmbiarpassword`
Source: Live CMS	`Source_CMS`	CMS to which the promotion management tool must connect. Value: Free form text Example: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_UserName`	User account that the promotion management tool must use to connect to the BI platform CMS. Value: Free form text Example: `Source_username=adminLCM`
	`Source_password`	Password of the user account. Value: Free form text Example: `Source_password=my_adminpassword1`

> **Note**
>
> Mandatory for SAP authentication.

> **Note**
>
> Mandatory for SAP authentication.

Parameter group	Parameter	Description
	`Source_authentication`	Indicates the authentication type to be used. Value: secEnterprise, secWinAD, secLDAP,secSAPR3. If not specified, `secEnterprise` is used. Example: `Source_authentication=secEnterprise`
	`Source_systemID` **Note** Mandatory for SAP authentication.	Required for SAP authentication only. Value: System ID Example: `Source_systemID=systemID`
	`Source_clientID` **Note** Mandatory for SAP authentication.	Required for SAP authentication only. Value: System ID Example: `Source_clientID=clientID`
Destination: LCMBIAR file	`exportLocation`	Specifies the location to place the LCMBIAR file after the objects have been exported and packaged. Value: Free form text. Must have `<.lcmbiar>` extension Example: `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Enables the encryption and decryption of BIAR files using a password . Value: Free form text Example: `lcmbiarpassword=validlcmbiarpassword`
Destination: Live CMS	`Destination_CMS`	CMS to which the tool must connect. Value: Valid CMS name Example: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	User account that the tool must use to connect to the BI Platform CMS. Value: Valid user name Example: `Destination_username=adminLCM`

Parameter group	Parameter	Description
	`Destination_password`	Associated password of the user account. Value: Valid password Example: `Destination_password=my_adminpassword1`
	`Destination_authentication`	Indicates the authentication type to be used. Value: secEnterprise, secWinAD, secLDAP, secSAPR3. If not specified, `secEnterprise` is used. Example: `Destination_authentication=secEnterprise`
	`Destination_systemID` **Note** Mandatory for SAP authentication.	Required for SAP authentication only. Value: System ID Example: `Destination_systemID=systemID`
	`Destination_clientID` **Note** Mandatory for SAP authentication.	Required for SAP authentication only. Value: Client ID Example: `Destination_clientID=clientID`
Job related	`JOB_CUID`	Instructs the tool to export all the objects in the job to the LCMBIAR file. Value: The CUID of the saved Management Job.
	`Override`	Used to selectively promote objects from a LCMBIAR file. When `true`: enables the user to override an existing job. When `false`: enables the user to create a new job with the name `<JOB_NAME>_<TIME_STAMP>` . Value: true or false Example: `Override=true`
	`forceOverride` Available in SP4	Used to override a job with the same name but not the same CUID. Value: true or false Example: `forceOverride=true`

Parameter group	Parameter	Description
	`Timeout` Available in SP4	Sets a timeout for promote action. Value: Time in seconds Example: `timeout=30`
Export related	`ExportDependencies`	Specifies the object dependencies that the tool gathers for exportation. Applicable only when used in conjonction with the `Source_CMS` flag. Value: true or false. If not specified the default is `false`. Example: `ExportDependencies=false`
	`ExportQuery`	Queries the LCM tool executes to get the required objects for export to the target CMS. Value: Free form text. Use the CMS query language format. Example: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Note** You can have any number of queries in one properties file, but they must be named as exportQuery1, exportQuery2.
	`ExportQueriesTotal`	Used to specify the number of export queries to execute. If you have x export queries and want to execute them all, you must set this parameter value to x. Value: positive whole number. If not specified the default is 1. Example: `ExportQuery1=<your sql statement> ExportQuery2=<your sql statement> ExportQueriesTotal=2`

Parameter group	Parameter	Description
	`BatchJobQuery`	Used in conjonction with `ExportQuery`. Creates and starts a job for each line returned by the job query. Job export queries can use "placeholders" that reference properties raised in the job query. The placeholder format is $b:PPTY$, where the property name is not case sensitive. The valid <PPTY> are:- "cuid" - "name" - "id" An error is raised if a placeholder is not recognized or raised by the job query. Value: Free form text Example: `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0` `exportQuery1= SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'" ,"SI_CUID='$b:CUID$'")`
	`LimitQueryBatchSize`	Restricts the number of returned objects to 1,000 by default. When this parameter is set to false, all queried objects will be returned. **Note** You can also explicitly set the new limit for the number of objects returned by the query using `select TOP <number>` Value: true or false. If not specified the default is true. Example: `LimitQueryBatchSize=true`
Log related	`consolelog`	Used to display the complete log of the command executed by the user in the command log. Value: true or false. If not specified the default is `false`. Example: `consolelog=true`

Parameter group	Parameter	Description
	`ResultFileName`	The name of the file on the local file system when the parameter `consolelog` is used. Value: job result file path Example: `ResultFileName=C:\Logs\ResultFile.txt`
	`LogFileName` Available in SP4	Enables the user to specify a fixed path to use for the log file. Value: log file path Example: `LogFileName=C:\Logs\LogFile.log`
Object selection	`Selected_CUIDS`	Enables the user to selectively promote objects (reports,users,universes etc.) along with their dependencies from an LCMBIAR file instead of promoting the entire file. Value: CUIDs of objects within the lcmbiar file that are to be selectively promoted
	`selectUser` Available in SP4	Filters users based on third party authentication (LDAP, SAPR3, WindowsAD...). Value: all, none, excludeTP or onlyTP. If not specified the default is `all`. Example: `selectUser=excludeTP`
	`selectGroup` Available in SP4	Filters user groups based on third party authentication (LDAP, SAPR3, WindowsAD...). Value: all, none, excludeTP or onlyTP. If not specified the default is `all`. Example: `selectGroup=onlyTP`
Security	`IncludeApplicationSecurity`	Instructs the tool to export or import the security associated with selected applications. Value: true or false. If not specified the default is `false`. Example: `IncludeApplicationSecurity=true`
	`IncludeSecurity`	Instructs the tool to export or import the security associated with selected objects and selected users. If access levels are used this will also export/import them. Value: true or false. If not specified the default is `false`. Example: `IncludeSecurity=true`

Parameter group	Parameter	Description
Comments	`IncludeComments`	Instructs the tool to export or import the comments associated whith selected objects. Value: true or false. If not specified the default is `false`. Example: `IncludeComments=true`
Federation Jobs	`IncludeFederationJobsRelationship`	Instructs the tool to keep the relationships of Federation Jobs (Replication Lists and Remote Connections). When set to false, replicated objects will become regular objects and the federation flag will be removed. This can be helpful when the replicated object is the only object available and the source object is no longer available. Value: true or false. If not specified the default is `true`. Example: `IncludeFederationJobsRelationship=false`

15.6.3.6 Rollback

You can revert the promoted job on the destination system through *Promotion Management* tool.

If you have promoted a job through *Promotion Management* tool, for example, to update BI 4.2 SP07 to BI 4.3, and if you want to revert this change later, then you can use the command line parameters, defined in Command line parameters by promotion scenario [page 578] and perform the rollback operation.

When you are performing the rollback operation, you have to provide a properties file that specifies the promotion order as follows:

- Promotion action type: rollback
- Login credentials to the CMS hosting the promotion management tool (previously called the lifecycle management tool LCM).
- Login credentials for the source CMS.
- Login credentials for the destination CMS.
- Other parameters required to successfully promote the CMS, for example security or dependencies parameters.

You can include other optional parameters that can specify particular promotion needs. These optional parameters are described in List of all the command line parameters [page 591].

You can refer to the sample properties file below to perform a rollback operation:

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
```

```
LCM_authentication=secEnterprise
```

> **Note**
>
> You can find the `job_cuid` for a promoted job at *CMC Home* > *Promotion Management* > *Properties*.

The following table lists the mandatory parameters required for a successful properties file for a promotion LCMBIAR file to live CMS:

Parameter group	Parameter	Description
Action type	`action`	Operation that the CLI must perform. Value: rollback Example: `action=rollback`
Job Related	`job_cuid`	Instructs the tool to export all the objects in the job to the LCMBIAR file. Value: The CUID of the saved Management Job. Example: `job_cuid=AWWxyVk5fkFKjtQnRAygAYg`
LCM Node	`LCM_CMS`	CMS for the promotion management tool. Value: Free form text Example: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Account user name that the tool must use to connect to the promotion management tool CMS. Value: Free form text Example: `LCM_userName=adminLCM`
	`LCM_password`	Password of the user account. Value: Free form text Example: `LCM_password=my_adminpassword1`

Parameter group	Parameter	Description
	`LCM_authentication`	Authentication type for the user account Value: Type of Authentication Example: `secEnterprise`

15.6.4 Sample properties file

The following is a sample `properties` file:

Example

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<CMS name:port number>
LCM_userName=<username>
LCM_password=<password>
LCM_authentication=<authentication>
LCM_systemID=<ID>
LCM_clientID=<client ID>
Destination_CMS=<CMS name:port number>
Destination_userName=<username>
Destination_password=<password>
Destination_authentication=<authentication>
Destination_systemID=<ID>
Destination_clientID=<client ID>
lcmbiarpassword=<password>
```

> **Note**
>
> If the `properties` file does not have any personal information, the LCM CLI will prompt for the same in the console.

15.7 Using the Promotion Management Wizard

Promotion Management Wizard allows you to copy business intelligence (BI) resources from one repository to another easily, in a few clicks.

Promotion Management Wizard supports the following promotion scenarios:

- Export a BI resource from a source system to an LCMBIAR file.
- Replicate a BI resource from a source system to a destination system.
- Import an LCMBIAR file to a destination system.

With Promotion Management Wizard, you can now promote the full content of a repository or selective content of a repository, without using the command line. The easy-to-use graphical interface of Promotion Management Wizard facilitates your work as an administrator.

For additional information regarding the best practices for Promotion Management Wizard, refer to SAP Note 2531264.

> ⚠ Caution
>
> Promotion Management Wizard doesn't support rollback. This means that after promoting BI resources, you can't restore the destination system to its previous state.

> ⓘ Note
>
> Make sure to review the memory value before you start promoting objects. The Xms value needs to be lesser or equal to the Xmx value.

> ⓘ Note
>
> If you have QaaWs objects, you must set up the destination system properly.

> → Tip
>
> To increase performance, disable auditing and monitoring in the CMC of the destination system. For more information, see Business Intelligence Platform Administrator Guide > Auditing.

15.7.1 To exclude objects from promotion

You can choose the objects from the list provided below and exclude them from a promotion job to save disk space and reduce the migration time.

Context

A promotion job migrates every BI asset from the source to the destination system. As a result, the assets, which are specific to the source system and not useful in the destination system, also gets migrated. To exclude BI assets from promotion, follow the steps below.

Procedure

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Open *PromotionManagementWizard.ini* in a text editor.
3. Search and locate the string *# List of kinds to exclude automatically from full/selective export.*.
   You'll find the code `-Dcom.sap.businessobjects.pmw.exclude.kind={}` below the string.
4. Refer to the list of objects below and add the objects to be excluded between the `{}`.
5. Save the file.

Results

The objects mentioned in the code will be excluded when you run a promotion job.

Refer to the table below for the list of objects that can be excluded from a promotion job.

CustomMapped Attributes	DFS.Parameter	Discussions	GDPR Object
LCM JOBS	LCM Overrides	LCM Scan History	LCM Settings
LANDSCAPE	LANDSCAPE Connection	LIVE Office	MoN.MBEAN Config
MON.ManagedEntity Status	MON.MonAppDataStore	Mon.Probe	Mon.Subscription
NotificationScheduleObject	Override entry	PlatformSearchApplication Status	PlatformSearchContentExtractor
PlatformSearchContentStore	PlatformSearchIndexEngine	PlatformSearchQueue	PlatformSearchScheduling
PlatformSearchSearchAgent	PlatformSearchServiceSession	TaskTemplate	VisualDifferenceComprator
XL.XcelsiusApllication	busobjectreporter	Explorer	Lumira Extensions

15.7.2 When to use the Promotion Management Wizard

There are several different options available to you for promotion management. This table helps you determine whether Promotion Management Wizard is the most appropriate solution for your needs.

Different options for promotion management

	Promotion Management Wizard	Promotion Management using the Command Line option	Promotion Management within the Central Management Console
Purpose	One shot promotion	Automation	Project
Promotion Scope	Important number of BI resources	Important number of BI resources	A few BI resources
Job	No possibility to create a job that can be rerun by the job server	Possibility to create a job run by the job server	Possibility to create a job run by the job server

> **Note**
>
> LCMBIAR files are compatible with each promotion management option, regardless of the promotion management option you select.

15.7.2.1 Defining the promotion management settings

Procedure

1. Specify the promotion management settings you require. Information to help you is provided here:

Setting	Description
Temporary Folder	**Note** Make sure you allocate enough free space in the Temporary Folder. The amount of free space needs to be at least twice the amount of space needed.
Log Location	The log location is defined by default. You can change the log location later. The modifications are immediately taken into account in the promotion management settings.
Log Level	You can set the Log Level to the following levels: • Default • Low

Setting	Description
	• Medium • High The Log Level is set to "Default" unless you change it.
Language	You can set Promotion Management Wizard to your preferred language.

2. Click *Next*

15.7.3 Scenario

Promotion Management Wizard supports three types of promotion scenario:

- Live system to LCMBIAR: You copy objects from a live CMS to an LCMBIAR file.
- Live CMS to live promotion: You copy objects from a live CMS source system to a live CMS destination system.
- LCMBIAR to live system: You import objects from an LCMBIAR file to a live CMS destination system.

15.7.3.1 Promoting objects from a live CMS source system to an LCMBIAR file

Context

To promote objects from a live CMS to an LCMBIAR file:

Procedure

1. Select *Export*.
2. To define the Source CMS, perform one of the following:
   - To use the central CMS as the Source CMS, check the box *Make the Central CMS as the Source CMS*.
   - In the Source section, enter the following information:
     - CMS Name
     - User
     - Password

- Authentication

3. In the *Destination* field, click *Choose* to select the location of the LCMBIAR file.
4. (Optional) Enter a password to encrypt the LCMBIAR file.

> **Note**
>
> If you encrypt the LCMBIAR file, the promotion process takes more time.

5. Click *Next* to select the objects you want to export.

15.7.3.2 Promoting objects from a live CMS source system to a live CMS destination system

Context

To promote objects from a live CMS source system to a live CMS destination system:

Procedure

1. Select *Promote*.
2. To define the Source CMS, perform one of the following:
   - To use the central CMS as the Source CMS, check the box *Make the Central CMS as the Source CMS*.
   - In the Source section, enter the following information:
     - CMS Name
     - User
     - Password
     - Authentication
3. To define the Destination CMS, perform one of the following:
   - To use the central CMS as the Destination CMS, check the box *Make the Central CMS as the Destination CMS*.
   - In the *Destination* section, enter the following information:
     - CMS Name
     - User
     - Password
     - Authentication
4. Click *Next* to select the objects you want to copy from the source system to the destination system.

15.7.3.3 Promoting objects from an LCMBIAR file to a live CMS destination system

Context

To promote objects from an LCMBIAR file to a live CMS:

Procedure

1. Select *Import*.
2. To define the Destination CMS, perform one of the following:
   - In the *Destination* section, check the box *Make the Central CMS as the Destination CMS*.
   - In the *Destination* section, enter the following information:
     - CMS Name
     - User
     - Password
     - Authentication
3. In the *Source* section, click *Choose* to select the LCMBIAR file you want to import.
4. (Optional) Enter a password to encrypt the LCMBIAR file.

   > **Note**
   >
   > If you encrypt the LCMBIAR file, the promotion process takes more time.

5. Click *Next* to select the objects you want to import.

15.7.4 Objects

Promotion Management Wizard supports two types of content promotion:

- Full content promotion
- Selective content promotion

The table, below, explains each type:

Content Promotion Types	Content Promoted	Content Dependencies
Full content promotion	You promote all the following contents from the source system to the destination system: • Objects (users, documents, universes, connections, etc.) • Instances • Relationships between objects • Object security	Since all relationships are maintained, dependencies don't need to be evaluated. You go from the current Objects step directly to the Summary step.
Selective content promotion	You promote the content that you have selected from the source system to the destination system. The content can be the following: • Objects (users, documents, universes, connections, etc.) • Instances • Relationships between objects • Object security	Since you don't promote all the contents from the source system to the destination system, dependencies need to be evaluated.

15.7.4.1 Promoting the full content

Context

To promote the full content from the source system to the destination system:

Procedure

1. Select *Full content promotion*.

   All the objects are selected for the promotion.
2. Click *Next* to review the content you have selected.

15.7.4.2 About promoting selective content

Before you promote the selective content from the source system to the destination system, you need to define the Export Options. Defining export options enables you to retrieve settings specified on the source system that you want to promote to the destination system.

15.7.4.2.1 About Export Options

If you want to retrieve settings specified on the source system and promote them to the destination system, you need to define the following parameters in Export Options:

- Object Instances
- Object Dependencies
- Security
- Commentary
- Federation Jobs
- Conflict name resolution

Object Instances

Object Instances	Description
Export all instances of an object when the object is selected	You export the selected objects with all their instances.
Export only the recurring instances of an object when the object is selected	You export the selected objects with only their recurring instances. For example, if you have scheduled a weekly and a monthly refresh for a document, this document and its two recurring instances will be exported during the export.
Do not export object instances	You only export the selected objects. Their instances are not exported.

Object Dependencies

Object Dependencies	Description
Include dependencies when selecting objects	You export the selected objects with all their dependencies. **Note** The option is checked by default.

Object Dependencies	Description
Exclude dependencies when selecting objects	You only export the selected objects without all their dependencies.

Security

Security	Description
Include Object Security	You export the selected objects with their object security settings.
Include User Security	You export the selected objects with their user security settings.
Include Application Security	You export the selected objects with their application security settings.
Include top level security	You export the security settings defined in the root folder. **⚠ Caution** This option overwrites the security settings defined in the destination system. You should use this option sparingly.

Commentary

Commentary	Description
Include Comments	You export the selected objects with all their comments.
User group BI launch pad preferences	If you select the checkbox, then the BI Launchpad user group preferences of the source system are and the default preferences are set in the destination system.

User Group BI Preferences

User Group BI Preferences	Description
Overwrite User Groups BI preferences	If you select the checkbox, then the BI Launchpad user group preferences of the source system are and the default preferences are set in the destination system. **ⓘ Note** If you are promoting a Web Intelligence document that uses customization using a BIAR file, make sure to enable this option to import the customization.

Federation Jobs

Federation Jobs	Description
Include Federation Jobs relationship	You import the selected objects with their Federation Jobs relationships maintained.

Conflict name resolution

Conflict name resolution	Description
Conflict name resolution	If a selected object has the same name but a different CUID as an object in the destination system, a copy of the selected object will be created in the destination system. If you don't activate this option, the selected object with the same name but a different CUID as an object in the destination system will not be copied in the destination system.

15.7.4.2.2 Promoting selective content

Context

To promote the selective content from the source system to the destination system:

Procedure

1. Select *Selective content promotion*.
2. To define *Export Options*, click *Options*.
3. (Optional) Check *Apply Time Filter* to filter objects according to a date and time range.
4. Select the objects you want to export.
5. To evaluate the dependencies of an object, check the associated box below the dependencies icon

   > **Note**
   >
   > By default, the dependencies boxes are all checked. If you don't want to evaluate the dependencies of an object, uncheck the box.

6. Click *Next* to evaluate the dependencies.

15.7.5 Dependencies

Context

If you choose to promote selective content from the source system to the destination system, the dependencies of the selective content can be evaluated. The *Dependencies* step provides an overview of the selected objects identified as dependencies.

You can view the following information on the dependencies of the selected objects:

- Title
- CUID
- Date

You can select objects identified as dependencies:

Procedure

1. Depending on the level of detail you want to view, perform one of the following:
   - Click *Expand all* to view the details of each dependencies.
   - Click *Collapse all* to only view the dependent objects.
2. Select the dependencies you want to promote.

   > **Note**
   >
   > By default, the dependencies boxes are all checked. If you don't want to promote the dependencies of an object, uncheck the box.
3. Click *Next* to review the objects you have selected for the promotion.

15.7.6 Summary

Context

Before you perform the promotion, you need to review the objects you have selected for the promotion.

You can view the following information about each object:

- Title

- CUID
- Date

> ⚠ Caution
>
> Make sure all the objects you want to copy are included because once the promotion starts, you cannot cancel the promotion process. Promotion Management Wizard doesn't support rollback.

You can review objects:

Procedure

1. Depending on the level of detail you want to review, perform one of the following:
   - Click *Expand* to view the details of each object.
   - Click *Collapse* to view the parent of each object.

   > ⓘ Note
   >
   > The level of detail varies in the promotion results CSV file, depending on whether you select *Expand* or *Collapse*.
2. To make sure you have enough space in your hard drive for the promotion, review the *Minimum temporary space required*.
3. Click *Start* to promote the objects.

   After you start the promotion, you cannot cancel the process.

15.7.7 (optional) Properties file

You can configure the following parameters in the properties file of the Promotion Management Wizard:

- SSL settings
- Parameters

The properties file of the Promotion Management Wizard is located in:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

15.7.7.1 Configuring SSL settings

Context

If you use SSL, you need to configure the SSL settings of the Promotion Management Wizard in

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

Procedure

1. Open `PromotionManagementWizard.ini` in a text editor.
2. To activate the SSL mode, uncomment the lines that begin with "-D".
3. Enter the values for each setting.

Setting	Value
`-Dbusinessobjects.orb.oci.protocol`	The value: ssl **Note** Entering this value enables SSL communication.
`-DcertDir`	The location of keys and certificates
`-DtrustedCert`	The name of the trusted certificate file **Note** If you specify more than one file, separate your entries with a semicolon (for example, fileA; fileB).
`-DsslCert`	The SDK certificate
`-DsslKey`	The private key of the SDK certificate
`-Dpassphrase`	The location of the file that contains the passphrase for the private key
`-Dpsecert`	The PSE certificate file

Caution

Do not add or edit any other settings or values.

4. Save `PromotionManagementWizard.ini`

Example: SSL settings in `PromotionManagementWizard.ini`

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

15.7.7.2 Configuring parameters

Context

Depending on your needs, you can configure options in the Promotion Management Wizard property file located in:

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

Procedure

1. Open `PromotionManagementWizard.ini` in a text editor.
2. To activate the options, uncomment the lines that begin with "-D".
3. Enter the values for each parameter.

Parameter	Value
`-Dbusinessobjects.connectivity.directory`	The location of the connection server directory.
`-Dcom.businessobjects.mds.cs.ImplementationID`	`csEX` **Note** Do not change or edit this value.

Parameter	Value
`-Xms8g`	The memory value is set by default at 8 Gb. The Xms value must be lesser or equal to the Xmx value.
`-Xmx10g`	The memory value is set by default at 10 Gb. 10 Gb memory is enough for a repository of 65 000 objects.
`-Dbobj.biar.suggestSplit=512`	Default value (recommended) It is recommended to use the parameter `-Dbobj.biar.suggestSplit`. When you promote objects from a live CMS to an LCMBIAR file, this setting enables you to split the LCMBIAR file into multiple LCMBIAR files.
`-Dbobj.biar.forceSplit=768`	Default value (recommended) If the parameter `-Dbobj.biar.suggestSplit` can't be applied, the parameter `-Dbobj.biar.forceSplit` applies as a fallback solution.
`-Dcom.businessobjects.lcm.commit`	• KEEP_TS: Default value. This value enables you to keep the modification dates of the source. • LEGACY: The modification dates correspond to the execution date in the destination system. It is an existing behavior prior to 4.2 SP5
`-Dcom.sap.businessobjects.pmw.exclude.list`	This parameter enables you to permanently exclude objects when you promote objects from a source system to a destination system or when you export a source system to a LCMBIAR file. The value (CUID) can be an object (document, folder, etc.). If a folder is specified, all children of the folder will be excluded.

4. Save `PromotionManagementWizard.ini`.

Example: Promotion Management Wizard options in `PromotionManagementWizard.ini`

```
-Dbusinessobjects.connectivity.directory=C:\Program Files (x86)\SAP
BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
-Dcom.businessobjects.lcm.commit=KEEP_TS
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
```

```
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

15.7.8 Promotion Management Wizard on Linux

You can run Promotion Management Wizard on Linux.

Prerequisites

Before you start Promotion Management Wizard on Linux, ensure that the Java runtime is set in the system `PATH` variable.

Context

To start Promotion Management Wizard on Linux, perform the following steps:

Procedure

1. Open a shell and go to the installation directory, such as the following:
   `/usr/sap_bobj/enterprise_xi40`
2. Execute the following command:
   `./PromotionManagementWizard`

   Promotion Management Wizard starts.

   For more details about how to use SSH and X11 redirection, please consult your OS documentation.

16 Version Management

16.1 To manage different versions of an infoobject

Context

The version management application allows you to manage versions of BI resources that exist in the BI platform repository. It supports both Subversion and GIT version management systems. This section describes how to use the Version Management feature in the promotion management tool.

To create and manage different versions of an infoobject, complete the following steps:

Procedure

1. Launch the promotion management tool.
2. Right-click a job, select *VMS Actions*, and click *Add to VM*. (You can also click the *VMS Actions* tab and then click *Add to VM*.)

   > **Note**
   >
   > Clicking *Add to VM* results in the creation of a base version of the object in the VMS repository. A base version is required for subsequent check-in.

3. Click *Checkin* to update the document that exists in the VMS repository.
   The *Check-in Comments* dialog box is displayed.
4. Enter your comments, and click *OK*.
   The change in the version number of the selected infoobject is displayed in the VMS and Content Management System columns.
5. To obtain the latest version of the document from the VMS, select the required infoobject, and click *Get latest Version*.
6. To create a copy of the latest version, click *Create Copy*.
   A copy of the selected version is created.
7. Select *History* to view all the versions available for the selected resource.
   The *History* window is displayed. The following options are displayed:
   - *Get Version* - If there are multiple versions, and if you require a particular version of the BI resource, then you can select the required resource and click *Get Version*.
   - *Get Copy of Version* - This option allows you to obtain a copy of the selected version.
   - *Export Copy of Version* - This option allows you to obtain a copy of the selected version and save it to your local system.

16.1.1 Version Management application access rights

This section describes the application access rights for the version management application.

- You can set access rights to the version management application within the CMC.
- You can set granular application rights to various functions within the version management application.

To set specific rights in the version management application, complete the following steps:

1. Log into CMC and select *Applications*.
2. Double-click *Version Management*.
3. Click *User Security*, and select a user. You can view or assign security rights for the selected user.
4. The following version management specific rights are now available:
    - Allow Checkin
    - Allow Create Copy
    - Allow Delete Revision
    - Allow Get Revision
    - Allow Lock and Unlock
    - View and Version BOMM objects
    - View and Version Business Views
    - View and Version Calenders
    - View and Version Connections
    - View and Version Profiles
    - View and Version QaaWS
    - View and Version Report Objects
    - View and Version Security Objects
    - View and Version Universes
    - View Deleted Resources
5. If you wish to assign rights to a selected user, select the appropriate right and click *Assign Security*.

16.2 To manage different versions of BI resources

Context

The version management application allows you to maintain different versions of BI resources that exist in the BI platform repository. To facilitate this feature, the tool includes Subversion version control system.

To manage different versions of jobs or other infoobjects, complete the following steps:

Procedure

1. Log into the CMC application and select *Version Management*.
2. From the left panel of the *Version Management* window, select the folder to view the job or other infoobjects whose versions you want to manage.
3. Select the infoobjects and click *Add to VM*.

   > **Note**
   >
   > Clicking *Add to VM* results in the creation of a base version of the object in the Version Management System (VMS) repository. A base version is required for subsequent check-in.

4. On subsequent changes to the document and to version the incrementally changed document, click *Checkin*. This will update the document that exists in the VMS repository.

   The *Check-in Comments* dialog box is displayed.
5. Enter your comments, and click *OK*.
   The change in the version number of the selected infoobject is displayed in the *VMS Version* and *CMS (Central Management Server) Version* columns.
6. To obtain the latest version of the document from the VMS, select the required infoobject, and click *Get latest Version*.
   The last version from the VMS repository is imported to the CMS.
7. To create a copy of the latest version, click *Create Copy*.
   A copy of the selected version is created in the VMS and CMS repositories.
8. Select *History* to view all the versions available for the selected infoobject.
   The *History* window is displayed. The following options are displayed:
   - *Get Version* - If there are multiple versions, and if you require a particular version of the BI resource, then you can select the required infoobject and click *Get Version*.
   - *Get Copy of Version* - This option allows you to obtain a copy of the selected version.
   - *Export Copy of Version* - This option allows you to obtain a copy of the selected version and save it to your local system.
   - *Compare* - This option enables you to compare the metadata information of two versions of a job. For more information, see “Comparing different versions of the same job”.
9. Select an infoobject and click *Lock* to lock the infoobject,or *Unlock* to unlock the infoobject, or *Delete* to delete all versioned content from the VMS repository. Content in the CMS is not affected.

   > **Note**
   >
   > If you lock an infoobject, you cannot perform any action on that infoobject.

10. When the version in the CMS is newer than the version in the VMS, an indicator is displayed beside the updated infoobject. When you place the cursor on the indicator, the `The version in CMS is newer` tool tip is displayed.
11. To view the list of all checked in resources that exist in the VMS but not in the CMS, click *View Deleted resources*.
    Click any deleted resource to view the history of that resource. You can select a deleted resource, and click *Get Version* to view that particular version of the resource.

    Click *Delete* to permanently drop the object from the VMS repository as well.

> **Note**
>
> If you use *Get Version*, the resource is moved from the VMS missing file list to the CMS.

12. Select an infoobject, and click to view the properties of the infoobject.
    Alternatively, you can right-click the infoobject and perform steps 3 to 12.
13. You can search for BI assets in the *Version Management* application. You can use the options such as *Find All Fields*, *Find Title*, *Find Keyword*, and *Find Description* to do a specific search for faster results.

> **Note**
>
> The search functionality in *Version Management* application is contextual. This means that if you select a folder such as *Auditing* and enter a string to search a document, then the BI platform looks for the document only in the *Auditing* folder. Similarly, if you select *All Folders* and do a search, then the BI platform looks for the infoobject in every folder.

16.3 To use Git as the Version Management System

Context

You can set Git as yourVersion Management System and configure the settings from Central Management Console.

Procedure

1. In CMC Home page, select *Applications*.
2. Double-click on *Version Management*.
   The *VMS Settings* in *Version Management Settings* screen is displayed.
3. Choose *Git* from the *Version Management Systems* list.
   Git Settings and the required parameters are displayed.
4. Select a protocol and enter the value in the empty fields. Refer to the table below to understand more about each field.

UI Terms	Description
Protocol	Choose Local if Git is installed in your local system and choose HTTP(s) if Git is installed on a remote server.
Username	Enter the username of the server where Git is installed.

UI Terms	Description
Password	Enter the password to access the server where Git is installed.
Server URL	Enter the link to the server where Git is installed.
Workspace Directory	Enter the filepath where you want to save your workspace.
Server Repository Name	Enter a name for your server repository.
GIT Install Path	Enter the install directory of Git.

> **Note**
>
> If you want Git to be your default VMS, select *Use as Default VMS*.

5. (Optional) Select *Test VMS* to validate your VMS settings.
6. Select *Save*.
7. Go to *Servers* > *Servers List* and select *Restart Server* from the context menu of the *Adaptive Processing Server*.

Results

You've successfully configured Git as your Version Management System.

16.4 To compare different versions of the same job

Context

You can view the differences between two versions of the same job by completing the following steps:

Procedure

1. Log into the CMC application.
2. From the CMC home page, select *Version Management*.
3. From the Version management screen, select the job whose versions needs to be compared.
4. Click *History*.
   The History page appears which displays all the versions of the selected infoobject.
5. Select any two versions for comparison.
6. Click *Compare*.
   The comparison process starts and the differences are highlighted in orange color, and the missing objects are highlighted in red color.

7. Click *Save* to save the difference report.

17 Managing Applications

17.1 Disabling the GDPR Popup Message

Since the 4.2 SP5 release of the SAP BusinessObjects Business Intelligence Platform, the GDPR (Global Data Protection Regulation) disclaimer popup message is mandatory for all the users when they log into BI Platform web applications such as:

- BI Launchpad
- CMC
- Fiori BI Launchpad
- Open Document

Knowing the GDPR disclaimer message is mandatory, you have the option to turn off the display of this message.

> ⚠ Caution
>
> The GDPR disclaimer popup message **should not**, and **cannot** be disabled proactively. To ensure compliance with EU GDPR legislation, all the users must actively accept this message before proceeding.

Disabling the GDPR message for users logging into the BI Launchpad

1. On a default Tomcat installation, go to the properties file:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Create a new file called `<Infoview.properties>`, and type `<properties file>` in the custom path:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Create a new property entry for `<disclaimer.enabled>`, and set it to `<false>`:
   `disclaimer.enabled=false`
4. Save the file.
5. Restart Tomcat.

Disabling the GDPR message for users logging into the CMC

1. On a default Tomcat installation, go to the properties file:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`

Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`

2. Create a new file called `<CMCApp.properties>`, and type `<properties file>` in the custom path:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Create a new property entry for `<disclaimer.enabled>`, and set it to `<false>`:
   `disclaimer.enabled=false`
4. Save the file.
5. Restart Tomcat.

Disabling the GDPR message for users logging into the Fiori BI Launchpad

1. On a default Tomcat installation, go to the properties file:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Create a new file called `<FioriBI.properties>`, and type `<properties file>` in the custom path:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Create a new property entry for `<disclaimer.enabled>`, and set it to `<false>`:
   `disclaimer.enabled=false`
4. Save the file.
5. Restart Tomcat.

Disabling the GDPR message for Open Document

1. On a default Tomcat installation, go to the properties file:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Create a new file called `<OpenDocument.properties>`, and type `<properties file>` in the custom path:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Example: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Create a new property entry for `<disclaimer.enabled>`, and set it to `<false>`:
   `disclaimer.enabled=false`
4. Save the file.
5. Restart Tomcat.

17.2 Managing applications through the CMC

17.2.1 Overview

The *Applications* management area of the CMC allows you to change the appearance and functionality of web applications such as the CMC and BI launch pad, without doing any programming. You can also modify access to applications for users, groups, and administrators by changing the rights associated with each one.

In this section, you'll find contextual information, procedures, and instructions on how to manage various settings. The following applications have settings that can be modified through the CMC:

- *Alerting Application*
- *Analysis Office Runtime*
- *Authorization Server Configuration*
- *Authorized URL Configuration*
- *BI Administrators' Cockpit*
- *BI launch pad*
- *BI workspaces*
- *Central Management Console*
- *BI Commentary Application*
- *Crystal Reports Configuration*
- *HANA Authentication*
- *Information Design Tool*
- *Information Steward Application*
- *BI Admin Studio*
- *Multitenancy Management Tool*
- *Open Document*
- *Platform Search Application*
- *Promotion Management*
- *Recycle Bin Application*
- *RESTful Web Service*
- *Translation management tool*
- *Version Management*
- *Visual Difference*
- *Web Intelligence*
- *Web Service*
- *Workflow Assistant*

17.2.2 Common settings for applications

17.2.2.1 Setting user rights on applications

You can use rights to control user access to certain features of applications. The *Applications* area in the CMC lets you assign principals to the access control list for an application, view the rights that a principal has, and modify the rights that the principal has to an application. For more information about rights administration, see the *SAP BI platform Administrator Guide*.

17.2.2.2 To set the web application trace log level in the CMC

Context

To trace other web applications, you must manually configure the corresponding `BO_trace.ini` file.

Procedure

1. In the *Applications* area of the CMC, right-click an application and select *Trace Log Settings*.

   > ⓘ Note
   >
   > These applications have trace log settings: Fiorified BI launch pad, CMC, Open Document, Promotion Management, Version Management, Visual Difference, and Web Service.

   The *Trace Log Settings* dialog box appears.
2. Select a setting from the *Log Level* list.
3. Click *Save & Close*.
4. Restart the web application server.

Results

The new trace log level will take effect after the next web application logon.

Related Information

Trace log levels [page 627]

17.2.2.2.1 Trace log levels

The following trace log levels are available for BI platform components:

Level	Description
Unspecified	The trace log level is specified through other means (usually an `.ini` file).
None	No tracing occurs.
Low	The trace log filter allows logging error messages while ignoring warning and status messages. Important status messages are logged for component startup, shutdown, start request, and end request messages. This level is not recommended for debugging purposes.
Medium	The trace log filter is set to include error, warning, and most status messages. Least important or highly verbose status messages are filtered out. This level is not verbose enough for debugging purposes.
High	No messages are filtered. This level is recommended for debugging purposes. ⚠ Caution This trace log level significantly affects system resources, increasing CPU usage and consuming storage space.

17.2.3 Application-specific settings

17.2.3.1 Managing CMC application settings

17.2.3.1.1 Authentication and program objects

You can control the types of program objects users can run, and you can configure the credentials required to run program objects.

Be aware of the potential security risks associated with adding program objects to the repository. The level of file permissions for the account under which a program object runs will determine what modifications, if any, the program can make to files.

Enabling or disabling a type of program object

As a first level of security, you can configure the types of program objects available for use.

Authentication on all platforms

In the *Folders* management area of the CMC, you must specify credentials for the account under which the program runs. This feature allows you to set up a specific user account for the program, and assign it appropriate rights, to have the program object run under that account.

Alternatively, users who add program objects to information platform services can assign their own credentials to a program object and give the program access to the system. Thus, the program will run under that user account, and the rights of the program will be limited to those of the user. If you choose not to specify a user account for a program object, it runs under the default system account, which generally has rights locally but not across the network.

> ⓘ Note
>
> By default, when you schedule a program object, the job fails if credentials are not specified. To provide default credentials, select *CMC* in the *Applications* management area. On the *Actions* menu, click *Program Object Rights*. Click *Schedule with the following operating system credentials* and provide a default user name and password.

Authentication for Java programs

Information platform services allows you to set security for all program objects. For Java programs, information platform services force the use of a Java Policy File, which has a default setting that is consistent with the Java default for unsecured code. Use the Java Policy Tool (available with the Java Development Kit) to modify the Java Policy File, to suit your specific needs.

The Java Policy Tool has two code base entries. The first entry points to the SAP BusinessObjects Enterprise Java SDK and allows program objects full rights to all SAP BusinessObjects Enterprise JAR files. The second code base entry applies to all local files. It uses the same security settings for unsecured code as the Java default for unsecured code.

> ⓘ Note
>
> The settings for the Java Policy are universal for all Program Job Servers running on the same machine.

> ⓘ Note
>
> By default, the Java Policy File is installed to the Java SDK directory in the Information platform services install root directory. For example, a typical location on Windows is: `C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

17.2.3.1.1.1 To enable or disable a type of program object

Procedure

1. In the *Applications* area, select *Central Management Console*.
2. Click *Actions* > *Program Object Rights*.
   The *Program Object Rights* dialog box appears.
3. In the *Allow users to* area, select the types of program objects that you want users to be able to run.

   You can select *Run scripts/binaries* or *Run Java programs*.

   If you selected *Run Java programs*, you can select or clear the *Use impersonation* check box. This option provides the Java program a token with which to log on to Information platform services.
4. Click *Save & Close*.

Results

> **Note**
>
> If you upgrade to SAP BusinessObjects Business Intelligence Platform 4.3 Support Package 3, program object rights are denied for everyone by default. An administrator user (or any user in administrator group) can enable this.
>
> Under *Run Java programs*, there is a *Use impersonation* check box. In 4.3 Support Package 3, the *Use impersonation* check box is removed.

17.2.3.1.2 Registering processing extensions with the system

> **Note**
>
> This feature does not apply to Web Intelligence documents.

Before you can apply your processing extensions to particular objects, you must make your library of code available to each machine that will process the relevant schedule or view requests. Installing the BI platform creates a default directory for your processing extensions on each Job Server, Processing Server, and Report Application Server (RAS). It is recommended that you copy your processing extensions to the default directory on each server. On Windows, the default directory is `C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\ProcessExt`. On UNIX, it is the `sap_bobj/ProcessExt` directory.

> **→ Tip**
>
> It is possible to share a processing extension file.

Depending upon the functionality that you have written into the extension, copy the library onto the following machines:

- If your processing extension intercepts schedule requests only, copy your library onto each machine that is running as an Adaptive Job Server.
- If your processing extension intercepts view requests only, copy your library onto each machine that is running as a Crystal Reports Processing Server or RAS.
- If your processing extension intercepts schedule and view requests, copy your library onto each machine that is running as an Adaptive Job Server, Crystal Reports Processing Server, or RAS.

> ⓘ Note
>
> If the processing extension is required only for schedule/view requests made to a particular server group, you only have to copy the library to each processing server in the group.

17.2.3.1.2.1 To register a processing extension with the system

Procedure

1. Go to the *Applications* management area of CMC.
2. Select *Central Management Console*.
3. Click *Actions* > *Processing Extensions*.
   The *Processing Extensions: CMC* dialog box appears.
4. In the *Name* field, enter a display name for your processing extension.
5. In the *Location* field, type the file name of your processing extension along with any additional path information.
   - If you copied your processing extension into the default directory on each of the appropriate machines, just type the file name (but not the file extension).
   - If you copied your processing extension to a subfolder below the default directory, type the location as: `<subfolder>/<filename>`
6. Use the *Description* field to add information about your processing extension.
7. Click *Add*.

   > → Tip
   >
   > To delete a processing extension, select it from the *Existing Extensions* list and click *Delete*. (Make sure that no recurring jobs are based on this processing extension because any future jobs based on this processing extension will fail.)

8. Click *Save & Close*.
   The processing extension is registered with CMC.

Results

You can now select this processing extension to apply its logic to particular objects.

17.2.3.1.2.2 Sharing processing extensions between multiple servers

> **Note**
>
> This feature does not apply to Web Intelligence documents or reports created in SAP Crystal Reports for Enterprise.

If you want to put all processing extensions in a single location, you can override the default processing extensions directory for each Adaptive Job Server, Crystal Reports Processing Server, and RAS. First, copy your processing extensions to a shared directory on a network drive that is accessible to all of the servers. Map (or mount) the network drive from each server's machine.

> **Note**
>
> Mapped drives on Windows are valid only until you reboot the machine.

If you are running servers on both Windows and on UNIX, you must copy a .dll and an .so version of every processing extension into the shared directory. In addition, the shared network drive must be visible to Windows and to UNIX machines (through Samba or some other file-sharing system).

Finally, change each server's command line to modify the default processing extensions directory. To change the command line, go to the Servers tab in the CMC, select a server, and open its Properties page. Add `-report_ProcessExtPath <absolute path>` to the command line. Replace `<absolute path>` with the path to the new folder, using whichever path convention is appropriate for the operating system that the server is running on (for example, `M:\code\extensions`, `/home/shared/code/extensions`, and so on).

To modify the default processing extensions directory, use the CMC to stop the server. Then open the server's Properties to modify the command line. Start the server again when you have finished.

17.2.3.1.3 Managing CMC tab access

17.2.3.1.3.1 Delegated administration and CMC tab access

Typically, a BI platform system administrator manages a large number of documents, folders, users, servers, and other objects. However, large corporate environments may exceed the resources of a single administrator. A system administrator who wants to focus only on high-priority tasks can create delegated administrators and assign subsets of management tasks to them (for example, the administration of a department or tenant content). Unlike system administrators, delegated administrators perform a limited set of tasks and have fewer rights on objects in the system.

The default configuration of the Central Management Console allows users to access all available CMC tabs. The system administrator can manage CMC tab access to control which tabs are visible to principals (users or user groups). To improve the user experience and workflow of the delegated administrator, a system administrator may also hide any of the CMC tabs that a delegated administrator is not expected to use.

> ⚠ Caution
>
> Management of CMC tab access affects only the visual appearance of the CMC user interface. Hiding CMC tabs is not a security measure, because it does not set or modify security rights on objects within tabs. To ensure that users cannot perform unauthorized operations on unauthorized objects (for example, manage servers through the Central Configuration Manager or third-party software based on the BI platform SDK), you must set appropriate security rights on objects (such as server objects).

Related Information

To manage CMC tab access for other users [page 633]
To manage permission to configure CMC tab access for other users or user groups [page 635]

17.2.3.1.3.2 Working with CMC tab access

17.2.3.1.3.2.1 Managing CMC tab access for other users

A system administrator always has access to all CMC tabs. Use the following guidelines to administer the CMC tabs that principals can access:

- For a simplified management process and a reduced need for maintenance and troubleshooting, it is recommended that administrators manage CMC tab access on a user group level (instead of on a user level).
- For CMC tabs that have top-level folders, an administrator must grant access to a tab and grant the *View* right on the top-level folder of the tab. The following CMC tabs support top-level folders:
  - *Access Levels*
  - *Calendars*
  - *Categories*
  - *(Universe) Connections*
  - *Cryptographic Keys*
  - *Events*
  - *Federations*
  - *Folders*
  - *Inboxes*
  - *OLAP Connection*
  - *Personal Categories*
  - *Personal Folders*

- *Profiles*
- *Replication Lists*
- *Servers and Groups*
- *Temporary Storage*
- *Universes*
- *Users and Groups*
- *Web Service Query*

- For improved system security, only members of the Administrators group can access the following CMC tabs. As system administrators, members of the Administrators group can access any CMC tab regardless of CMC tab access permissions. CMC tab access permissions are designed to control access to CMC tabs for delegated administrators; that is, users other than members of the Administrators group.
  - *Auditing*
  - *Authentications*
  - *Cryptographic Keys*
  - *License Keys*
  - *Monitoring*
  - *Sessions*
  - *Settings*
  - *User Attribute Management*

> ⚠ Caution
>
> Management of CMC tab access affects only the visual appearance of the CMC user interface. Hiding CMC tabs is not a security measure, because it does not set or modify security rights on objects within tabs. To ensure that users cannot perform unauthorized operations on unauthorized objects (for example, manage servers through the Central Configuration Manager or third-party software based on the BI platform SDK), you must set appropriate security rights on objects (such as server objects).

17.2.3.1.3.2.1.1 To manage CMC tab access for other users

Procedure

1. Log on to the CMC.
2. On the *Users and Groups* tab, right-click a principal and select *CMC Tab Configuration*.

   > ⓘ Note
   >
   > If CMC tab access is unrestricted, the following message will be displayed: `Warning: CMC tab access is currently unrestricted. To restrict CMC access, click the "Application" tab, select "CMC," and set the CMC tab access to restricted. These settings take effect after CMC tab access is restricted.` You can still configure CMC tab access. However, the configuration will not take effect until you restrict CMC tab access.

   In the *Configure CMC Tab Access* dialog box, a table is displayed:

- or □ indicates which CMC tabs the principal can access.
- *Inherited* indicates that the tab access was inherited from its parent user group(s).
- *Explicit* indicates that the tab access was explicitly specified on the principal level.

3. Review the CMC tab access rights. To modify the rights, you can use the buttons on the toolbar:
   - Click *Grant* to explicitly grant access to a tab.
   - Click *Deny* to explicitly deny access to a tab.
   - Click *Inherit* to use an inherited access right.

   > ⓘ Note
   >
   > Clicking the buttons applies changes to the principal immediately.

4. When you are finished, click *Close*.

Results

The new effective tab access is displayed in the *Permission* column of the table.

Related Information

To restrict CMC tab access [page 637]

17.2.3.1.3.2.1.2 Inheritance of CMC tab access

CMC tab access rights and the permission to configure CMC tab access for other users or user groups are both applied and inherited in the same way as other BI platform security rights. If principals have no tab access explicitly specified, they will inherit the tab access of the user groups they are members of.

If a user is a member of two user groups, tab access is calculated in the same manner as all other BI platform rights are calculated. For example, if access to a CMC tab is granted in one of the groups and denied in the other, the principal will not be able to access the CMC tab.

> ⓘ Note
>
> - Modifying the CMC tab access right of a user group changes the same tab access for all users or user groups that inherit rights from the user group, if their CMC tab access is set to *Inherited*.
> - Tab access set on the user level always supersedes tab access inherited from user groups.

17.2.3.1.3.2.1.3 Delegated administrator user groups

You can create a set of delegated administrator user groups to simplify CMC tab management. To avoid configuring individual CMC tab access, you can make an existing user or user group a member of a delegated administrator user group. The following configuration is recommended, but it can be modified for specific business needs.

> **Note**
>
> Membership in multiple groups will result in the addition of rights, if the rights are set to *Inherited*.

Delegated Administrator User Group	Recommended Rights
System Administrators	Grant access to all tabs.
User Administrators	Grant access to *Access Levels*, *Folders*, *Inboxes*, *Personal Folders*, *Personal Categories*, *Query Results*, *Sessions*, and *User and Groups*. Set all other tabs to *Inherited*.
Content Administrators	Grant access to *Calendars*, *Categories*, *Events*, *Folders*, *Instance Manager*, *Personal Categories*, *Personal Folders*, *Profiles*, *Query Results*, and *Universes*. Set all other tabs to *Inherited*.
Server Administrators	Grant access to *Servers* and *Applications*. Set all other tabs to *Inherited*.

17.2.3.1.3.2.1.4 To manage permission to configure CMC tab access for other users or user groups

Context

In a large corporate environment, a system administrator may need to delegate CMC tab access management to a delegated administrator. Alternatively, in a multitenant system each tenant may have a delegated administrator responsible for managing CMC tab access for other users and user groups.

Procedure

1. Log onto the CMC.
2. On the *Users and Groups* tab, right-click a principal and select *CMC Tab Configuration*.
   In the *Configure CMC Tab Access* dialog box, the *Permission to configure CMC tab access for other users or user groups* is displayed for the principal.

   > **Note**
   >
   > If this permission is granted, the principal will be able to manage CMC tab access (only for tabs that the principal has access to) for users on which the principal has the *Securely Modify Rights* right. In

addition, the principal will be able to further delegate CMC tab access management to other users by granting the *Permission to configure CMC tab access for other users or user groups* to users on which the principal has the *Securely Modify Rights* right.

- or indicates whether the principal has permission to configure CMC tabs for other users or user groups.
- *Inherited* indicates that the permission was inherited from its parent user group(s).
- *Explicit* indicates that the permission was explicitly specified on the principal level.

3. Review the permissions to configure CMC tab access for other users or user groups. To modify the permissions, you can select one of the following settings from the list:
   - Click *Grant* to explicitly grant permission to manage CMC tab access for other users or user groups.
   - Click *Deny* to explicitly deny permission to manage CMC tab access for other users or user groups.
   - Click *Inherit* to inherit permission to managed CMC tab access for other users or groups.

   > ⓘ Note
   >
   > Selecting a setting from the list changes the permission of the principal immediately.

4. When you are finished, click *Close*.

Results

The new effective permission is displayed.

Related Information

Delegated administration and CMC tab access [page 631]
Inheritance of CMC tab access [page 634]

17.2.3.1.3.2.1.5 To add a Customization tab for a user or user group

Prerequisites

CMC tab access must be set to “Restricted” before you can add a *Customization* tab for a user or user group.

Context

Procedure

1. In the CMC, go the *Users and Groups* management area.
2. Right-click a user or user group and select *CMC Tab Configuration*.

   The *Configure CMC Tabs* dialog box appears, listing each CMC tab title and its permission level, for the user group.

   If the following warning message appears in red at the top of the dialog box, you must set CMC tab access to restricted before you can add a *Customization* tab:

   ```
   Warning: CMC tab access is currently unrestricted. To restrict CMC access, click
   the "Application" tab, select "CMC," and set the CMC tab access to restricted.
   These settings take effect after CMC tab access is restricted:
   ```
3. (If necessary) To set CMC tab access to restricted:
   a. In the *Applications* management area of the CMC, right-click *Central Management Console* and select *CMC Tab Access Configuration*.
   b. Under *CMC Tab Access*, select the *Restricted* option, and click *Save & Close*.
4. In the *Configure CMC Tabs* dialog box for the user group, for each CMC tab, select *Granted*, *Denied*, or *Inherited* in the list.
   Each time you change the permission for a tab, the Configure CMC Tabs dialog box updates the user group's permission to configure tab access for other users or user groups.
5. Click *Close*.

17.2.3.1.3.2.2 To restrict CMC tab access

Prerequisites

It is recommended that you first configure CMC tab access for principals, and then restrict CMC tab access. If you restrict tab access before configuring it, your users will not be able to access any CMC tabs until an administrator grants them access.

Context

To ensure consistency with previous versions of the BI platform, CMC tab access is initially unrestricted after the BI platform is installed, and any user who can access the CMC is able to access all available tabs. To prevent users from accessing tabs to which they have no access rights, a system administrator can restrict CMC tab access.

You can remove CMC tab access restriction in an urgent case, or to troubleshoot CMC tab access configuration (for example, if a delegated administrator cannot access an essential CMC tab).

Procedure

1. Log onto the CMC.
2. On the *Applications* tab, right-click *Central Management Console* and select *CMC Tab Access Configuration*.
   The *CMC Tab Access* dialog box is displayed.
3. Configure the CMC tab access rule.
   - To limit your users to access to tabs for which they have rights, select *Restricted*.
   - To allow your users to access all tabs, select *Unrestricted*.
4. When you are finished, click *Save and Close*.

Results

The CMC tab access rule is applied to the system.

Related Information

To troubleshoot CMC tab access [page 638]

17.2.3.1.3.2.3 To troubleshoot CMC tab access

Context

To prevent unauthorized access, or to troubleshoot a user's limited access to CMC tabs, you can troubleshoot a user's CMC tab access rights.

Procedure

1. Log onto the CMC as an administrator.

   > **Note**
   >
   > Ensure you have access to the tab that you want to troubleshoot, and that you have the *Securely Modify Rights* right on the user.

2. On the *Users and Groups* tab, right-click a principal and select *CMC Tab Configuration*.
   The *Configure CMC Tab Access* window is displayed.
3. Review the effective CMC tab access. You can explicitly grant or deny access to available tabs.

   If the CMC tab access is inherited, but the effective tab access does not match the user's needs:

a. Compile a list of all user groups that the selected principal is a member of.
b. Repeat steps 1-3 for every group that the user inherits tab access from.
c. Correct CMC tab access on the principal level or under the group level as needed.

> **Note**
>
> Performing this task on the group level affects CMC tab access for all users who are members of this user group, and all users who are members of user groups inherited from this user group, as long as the users have CMC tab access set to *Inherited*.

4. When you are finished, click *Close*.

Related Information

To manage CMC tab access for other users [page 633]
Inheritance of CMC tab access [page 634]

17.2.3.2 Managing BI launch pad settings

This section walks you through how you can manage the following settings in the BI launch pad:

- Changing display settings for the BI launch pad.
- Configuring RESTful URL details in Central Management Console for logon to the BI launch pad.
- Setting Authentication tab and CMS visibility in the BI launch pad.
- Configuring email link for *Contact Administrator* option in the BI launch pad.

17.2.3.2.1 Configuring RESTful URL details in CMC for logon to the Fiorified BI Launch Pad

After you install or upgrade BI 4.2 SP04 and above, you need to configure RESTful Web Services URL for a user to be able to log on to the fiorified BI launch pad.

Context

To configure RESTful Web Services URL details in CMC, perform the following steps:

Procedure

1. Logon to the CMC, as an Administrator.
2. Navigate to *Manage* > *Applications* > *RESTful Web Services* > *Properties*.
3. Provide the RESTful Webservice URL (hostname or fully qualified name where the RESTful Webservices are deployed).

17.2.3.2.2 Configuring proxy settings to enable Web Assistant in the Fiorified BI Launch Pad

After you install or upgrade to BI 4.2 SP5, you need to configure proxy settings for a user to be able to access Web Assistant in-app help in fiorified BI launch pad.

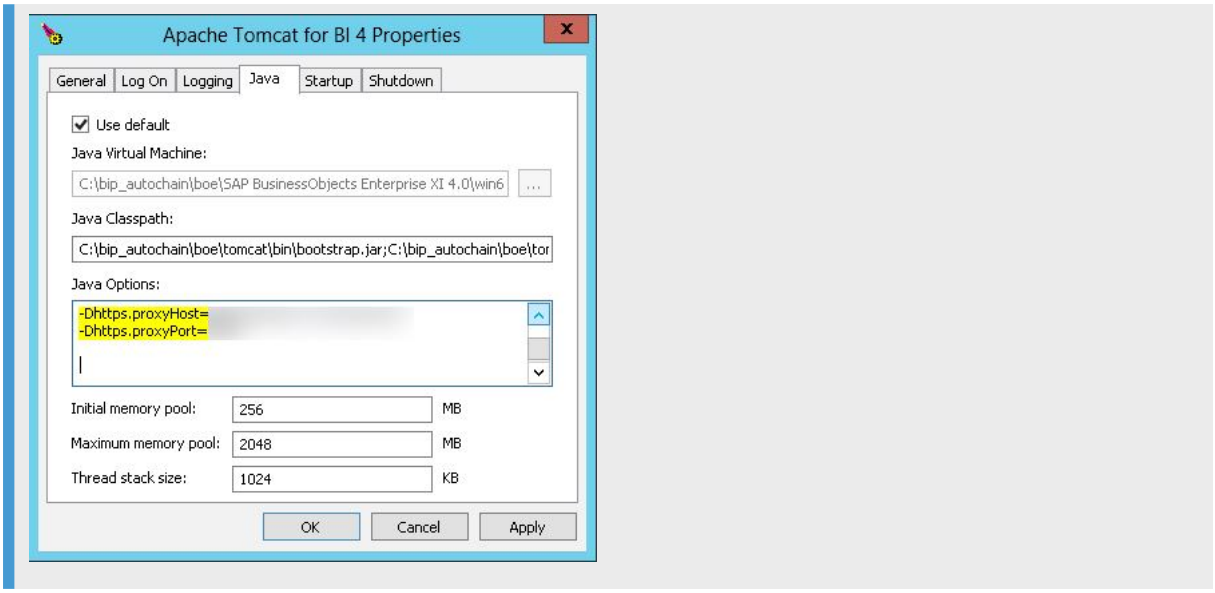
To configure proxy settings for web assistant in fiorified BI launch pad, perform the following steps:

Prerequisites:

You are connected to the internet.

1. Navigate to System Properties of the web server.
2. Add the `https.proxyHost` and `https.proxyPort` properties.

> ### Example
>
> OS: Windows, Web Server: Tomcat 8.5
>
> 1. Navigate to *Windows* > *Tomcat*.
>   The *Apache Tomcat for BI 4 Properties* window opens.
> 2. Choose the *Java* tab.
> 3. In the Java options field, append the following properties to the list:
>    ```
>    -Dhttps.proxyHost=<proxy_host>
>    -Dhttps.proxyPort=<proxy_port>
>    ```
> 4. Restart Tomcat.



17.2.3.2.3 Configuring email link for Contact Administrator option in the Fiorified BI Launch Pad

Context

To configure email link for the *Contact Administrator* option in the fiorified BI launch pad, perform the following

Procedure

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   If you have Tomcat version installed with BI platform, you can also access the following location: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Create a new file using Notepad and save the file with the following name: 'FioriBI.properties'.
3. Modify the following property in the file: `admin.user.email=administrator@bilp.com`, to include the email id of the administrator.

17.2.3.2.4 Setting Authentication tab and CMS visibility in the Fiorified BI Launch Pad

Context

To set Authentication tab and CMS visibility in the fiorified BI launch pad, perform the following:

Procedure

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   If you use Tomcat installed with BI platform, you can also access the following location: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Create a new file using Notepad and save the file with the following name: 'FioriBI.properties'.
3. To include the authentication options on the BI launch pad logon screen, add the following: `authentication.visible=true`.

   Replace <authentication> with default Authentication types: “secEnterprise, secLDAP, secWinAD, secSAPR3”.
4. To change the default authentication type, add the following: `authentication.default=<authentication>`.
5. To prompt users for the CMS name on the BI launch pad logon screen, add the following: `cms.visible=true`.
6. Save and close the file.
7. Restart your web application server.

17.2.3.2.5 To change display settings for BI launch pad

Procedure

1. Go to the *Applications* area of the CMC, and double-click *BI launch pad*.
   The *BI Launch Pad Properties* dialog box appears.
2. To enable filters for scheduling, select the *Show the "Filters" tab on the Schedule page* check box.

   This setting controls whether users can enter record or group selection formulas when scheduling a Crystal report.
3. Click *Save & Close*.

17.2.3.3 Managing Web Intelligence settings

You can control which features your users have access to for Web Intelligence documents by setting properties for the Web Intelligence application.

17.2.3.3.1 To modify display settings for Web Intelligence

Procedure

1. Go to the *Applications* area of the CMC and select *Web Intelligence*.
2. Click *Manage* > *Properties.*
   The *Properties* dialog box appears.
3. Define any of the following display options.

Option	Description
Changed data display options > *Dimensions and details*	Use the options in this area to define how added data appears in reports; change the font style, text color, and background color. A cell preview automatically shows your changes. Click *OK* when you are finished.
Changed data display options > *Fluctuating values (numerical measures)*	Use the options in this area to modify and format the page heading; change the font style, text color, and background color. A cell preview automatically shows your changes. Click *OK* when you are finished.
Embedded image properties	Enter the maximum embedded image size.
Geographic Maps Support	Enable or disable geographic maps support in Web Intelligence.
Quick display mode properties	In the appropriate fields, enter the maximum vertical records, maximum horizontal records, minimum width of page, minimum height of page, right padding value, and bottom padding value.
Auto-save Settings	Set the interval at which documents are autosaved. This interval is reset each time a document is saved manually or automatically. The autosaved document is also deleted when you close a document manually.
Automatic Refresh	Enables automatic refreshing of Web Intelligence documents when the Web Intelligence document property *Auto-refresh* is selected. For details, see the *SAP BusinessObjects Web Intelligence User Guide*.
Auto-Merge	Enables automatic merging of dimensions when the Web Intelligence document property *Auto-merge dimensions* is selected. For details, see the *SAP BusinessObjects Web Intelligence User Guide*.

Option	Description
Automatic Document Refresh on Open Security Right Setting	Clear this option to enable Web Intelligence to refresh documents automatically on opening, without enabling *Refresh on open* in the Web Intelligence document properties. Selecting this option selects the security right *Documents - disable automatic refresh on open*.
Smart View	This option determines which document version is displayed when users open documents in Web Intelligence. • View Latest Instance The latest instance of the object is opened. For example, if a document is scheduled for a refresh every hour, and the document was last saved and closed five hours ago, the latest instance is opened. • View Object The document is opened in the same state as when it was last saved, irrespective of any scheduled refreshes that might have occurred.
JavaScript	Your selection here defines the rendering of cells with the Read content as HTML or Read content as Hyperlink in Web Intelligence documents: • *Disable JavaScript and enable hyperlinks and only the HTML elements used by Web Intelligence* This default option enables hyperlinks and the limited set of HTML elements required for Web Intelligence functions. It removes JavaScript and the other HTML elements from the documents. • *Enable only HTML elements defined on the Authorized HTML Elements page* This option enables only the HTML elements and attributes that you specify on the *Authorized HTML Elements* page. • *Enable JavaScript, HTML elements and hyperlinks* This option enables all JavaScript, HTML elements, and hyperlinks. Whenever you change the option, to see the changes in Web Intelligence, log off and log onto the application. **⚠ Caution** • Web Intelligence enables embedded JavaScript/HTML code in document cells thanks to its formula capabilities. This code can be enabled or disabled in the Central Management Console. However, by authorizing JavaScript, HTMLs and hyperlinks, you acknowledge the risk that you are exposing yourself to Cross-Site Scripting. Cross-Site Scripting allows attackers to alter web sites or execute code on other systems. This vulnerability affects products such as internet browsers when they are running scripts. The majority of Cross-Site Scripting attacks result from insecure programming on the target system. • The code can be fine-tuned by authorizing HTML tags and attributes in *BI Admin Studio* > *Applications* > *HTML Elements*. However, SAP is not responsible for the compatibility of this code and its possible side effects. For example, your code might require some adaptation due to browser updates, JavaScript version support or the way the code is dynamically embedded in the web page. The code might require adjustments to run in that new context.

Option	Description
Content Alignment for New Documents	Use these options to define if new document's content must be aligned right-to-left, left-to-right or if it must depend on user's preferred viewing locale and/or product locale.
Features Toggle	Use this text field to enter toggles to enable preview features. These toggles may also be used in SAP Notes to modify default behavior. This list of toggles must be entered as a JSON-format list. Administrators can raise or reduce the row limit for a widget category or for all widgets, see SAP Note 3599785. **Note** Increasing the row limit has an impact on the ideal data flux and performance.

4. Click *Save & Close*.

> **Note**
>
> To revert your selection to the default display variables, click *Reset*.

17.2.3.3.2 Custom Elements services

Custom Elements are visualizations whose rendering is delegated to third-party services by Web Intelligence.

In Web Intelligence documents, Custom Elements are integrated and displayed like any other report element (chart, table, etc.). Custom Elements services must be configured in the CMC first so that end users can visualize Custom Elements in Web Intelligence documents.

Since your data will be transferred between the BOE server and the custom elements third-party server, we recommend deploying the Custom Elements server on your intranet. If not possible, then we recommend using exclusively HTTPS, when accessing the Custom Elements server.

> **Caution**
>
> The Custom Elements service you deploy adds code to Web Intelligence, and can generate potential security issues such as cross-site scripting. Cross-site scripting allows attackers to run code and execute scripts on other users' computers. A security warning asks for your explicit consent before your deploy you Custom Elements service. Your consent is mandatory to deploy the Custom Elements service.

Migration

When migrating a Web Intelligence document from a CMS to another, the Custom Elements service used to create content in this document will need to be re-created in the new CMS, with the same name. If the Custom Elements service is not re-created (with the same name) in the new CMS, then the Custom Elements in the migrated document are no longer modifiable.

17.2.3.3.2.1 To add a custom elements service

For end users to be able to use custom elements, you as an administrator first need to specify the third-party service that handles the rendering. By default, no custom elements service is activated. This setting is optional and needs to be enabled in the CMC.

Prerequisites

You have added the custom service URL to the list of trusted URLs. If you haven't, check the To add trusted URLs to the Authorized URLs list [page 652] section.

Procedure

1. Open the Central Management Console.
2. Click *Applications*.
3. Right-click on *Web Intelligence*.
4. Click *Properties*.
5. Click *Custom Elements*.
6. Click *Add Service*.
7. Give the service a name.

   > ⚠ Caution
   >
   > The name of the service will be displayed as is in Web Intelligence clients and has to be unique. You cannot reuse a service name that already exists. If you modify the name of a service, it will no longer be possible to modify the custom elements created with this service in Web Intelligence documents.

8. Enter a URL with the port number.
9. Click *Test*.
10. Select a *Media Type*.

    Web Intelligence is capable of consuming either HTML or bitmap media types. The preferred media type is HTML (text/html), which allows interactivity in Web Intelligence clients and a better user experience. Bitmap media types can be .PNG (image/png), .JPG (image/JPG) or .GIF (image/gif).

11. Enter the *Image DPI*.

    > ⓘ Note
    >
    > This is the resolution of the bitmap images generated by the service. A bitmap format is necessary for the publication of Web Intelligence reports as PDF or Excel files, where custom elements are represented as pictures. Without a bitmap format, these publications will show an empty block instead of the expected custom element.

12. Click *OK*.

> **Note**
>
> You can use several custom elements services at the same time. A single service can supply multiple custom elements.

Related Information

Authorizing URLs [page 651]

17.2.3.3.3 Parallel Data Provider Refresh

Parallel Data Provider Refresh improves data refresh performance in Web Intelligence documents that contain multiple data providers.

To refresh queries in parallel, Web Intelligence spreads all data providers on several threads. This feature is activated by default, and Web Intelligence can refresh up to 64 queries in parallel. Data providers based on relational, OLAP, and BICS connections are supported, as well as personal data providers (text files, FHSQL).

> **Restriction**
>
> Excel data providers are not supported.

You can decrease that value in the Central Management Console if the hardware running Web Intelligence does not support such a workload. Make sure that your hardware has enough cores to guarantee optimal performance.

Two global parameters are available in the Central Management Console:

- *Maximum Parallel Queries per document*: Set the maximum number of data providers Web Intelligence can refresh in parallel per document. The default value is set to 64.
- *Enable Parallel Queries for Scheduling*: Enable or disable the parallel query processing when scheduling documents. This option is enabled by default.

We also encourage you to fine-tune each database connection with a parameter that lets you specify the number of queries that can be run in parallel. This parameter, called Maximum parallel queries, is available:

- In the Central Management Console or Information Design Tool for OLAP and BICS connections.
- In Information Design Tool for relational connections.

For each connection, the number of data providers that can be refresh in parallel is set to 4 by default. The database administrator can change this value according to the database hardware. For text files however, the default value is set to 1.

Example

In this example, all default values have been kept and each connection supports a maximum of 4 parallel refresh jobs.

Connection	Number of Data Provider to Refresh
2 OLAP connections	6 (5 on Connection 1, 1 on Connection 2)
1 Relational connection	2
1 BICS connection	2
Excel files from a personal data provider	2

Both Excel files are refreshed sequentially as they are not supported by the parallel data provider refresh feature.

Four of the data providers of the first OLAP connection are refreshed in parallel on threads 1, 2, 3 and 4. The fifth one is queued and will be processed after one of the data provider (of any connection) has been refreshed, while the one coming from the second OLAP connection is refreshed on thread 5 since it is from a different connection.

The four data providers of both relational and BICS connection are refreshed in parallel on threads 5, 6, 7 and 8.

> ⓘ Note
>
> Whenever there are more data providers of the same type than the defined value, they are queued and wait for other data providers to finish.

Related Information

To modify the number of data providers refreshed in parallel per document [page 648]
To modify the number of data providers refreshed in parallel for a specific OLAP connection [page 649]

17.2.3.3.3.1 To modify the number of data providers refreshed in parallel per document

Context

Procedure

1. On the CMC home screen, click *Servers*.
2. Click *Web Intelligence Services*.
3. Right-click *Web Intelligence Processing Server* and click *Properties*.
4. In the *Maximum Parallel Queries* entry field, enter a number.

   The possible values range from 0 to 64.

   > ⓘ Note
   >
   > If you enter 0, you disable the parallel data provider refresh function.

17.2.3.3.3.2 To disable parallel query processing for scheduling

Context

Procedure

1. On the CMC home screen, click *Servers*.
2. Click *Web Intelligence Services*.
3. Right-click *Web Intelligence Processing Server* and click *Properties*.
4. Uncheck *Enable Parallel Queries for Scheduling*.

17.2.3.3.3.3 To modify the number of data providers refreshed in parallel for a specific OLAP connection

Context

Procedure

1. On the home screen, click *OLAP Connections*.
2. Browse the connection you want to configure and right-click it.
3. Select *Organize* > *Edit*.
4. In the *Maximum Parallel Queries* entry field, enter a number.
   The possible values range from 1 to 64.

   > **Note**
   >
   > If you enter 1, data providers will be refreshed sequentially.

17.2.3.3.4 Protection for CSV exports

Web Intelligence provides a security measure to prevent command injection when users open a CSV file generated from a document in Microsoft Excel. You can disable this protection for CSV exports.

By default, Web Intelligence adds a space before the following characters at the export to CSV or a CSV archive:

- = (Equal)
- + (Plus)
- - (Minus)
- @ (At)

The additional space prevents the values that contain these characters from being executed as commands and, consequently, causing a security issue on your system.

Related Information

To disable protection for CSV exports [page 651]

17.2.3.3.4.1 To disable protection for CSV exports

If you want to disable the default security measure in Web Intelligence that prevents command injection when users open an exported CSV file in Microsoft Excel, modify the corresponding registry key.

Context

Set the value of the `EscapeCharactersForCSVExport` registry key to false to disable the security measure. By default, the registry key is not present and its value is true so you may need to create it to set the value to false.

The change takes effect after Web Intelligence users close and open the application again.

Procedure

Change the registry key, as follows:

- In Windows, on the server machines and client machines, set the registry key to false: `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.
- In UNIX, on the server machines, in `$installdir/setup/boconfig.cfg`, set the registry declaration key to false `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.

17.2.3.3.5 Authorizing URLs

Web Intelligence use URLs for:

- Hyperlinks in the document
- Hyperlinks in prompt hints
- Background picture
- OData data source
- Custom elements or external extensions

These URLs can potentially create security threats.

As an administrator, you must build in the Central Management Console a list of trusted URLs that users can use. This list controls the use of these URLs in Web Intelligence.

17.2.3.3.5.1 To add trusted URLs to the Authorized URLs list

Whenever you want to use a URL in Web Intelligence as a hyperlink in the document or a prompt hint, a background picture, an OData data source, or a new custom service or external extension, you must authorize it first.

Procedure

1. On the Central Management Console home screen, click *Applications*.
2. Select *Web Intelligence*.
3. In the context menu, select *Properties*.
4. Select the *Authorized URLs* section.
5. Click the *Add a new URL* button to add a trusted URL.
6. In the *Authorized URL* field, specify a unique URL, with its protocol, hostname and port.

   > → Tip
   >
   > You can type the * character to authorize any URL for hyperlink or background picture or OData data source. You then need to click the *I accept the risk* checkbox to confirm that you understand the potential risk to enable all URLs.

7. If the entered URL is an URL to an extension or custom element service that can be accessed through a proxy, you can check the *If this URL is used for a custom element or an extension that requires a proxy, enter its server and port* checkbox to set this proxy server and port.
8. Click *OK*.

17.2.3.3.5.2 To remove URLs from the Authorized URLs list

You may want to remove some URLs from your list of Authorized URLs, if they are no more trusted or if you want to clean this list.

Procedure

1. On the *Central Management Console* home screen, click *Applications*.
2. Select *Web Intelligence*.
3. In the toolbar or its context menu, select *Properties*.
4. Select the *Authorized URLs* section.
5. Select to URLs to remove from the list by clicking them in the list. You can use the [Ctrl] and [Shift] keys to multi-select them.
6. In the toolbar, click *Remove the selected URL(s)*.

7. Click *OK*.

17.2.3.3.5.3 To disable and enable trusted URLs

You may want to temporarily disable some URLs from your list of Authorized URLs and latter enable them back. When an URL is disabled, it is no more allowed in Web Intelligence.

Procedure

1. On the *Central Management Console* home screen, click *Applications*.
2. Select *Web Intelligence*.
3. In the toolbar or its context menu, select *Properties*.
4. Select the *Authorized URLs* section.
5. Select the URLs to enable or disable from the list by clicking them in the list. You can use the [Ctrl] and [Shift] keys to multi-select them.
6. In the toolbar, depending on the action to perform, click *Disable the URL(s)* or *Enable the URL(s)*.
7. If you have selected to disable URL(s), click *OK* to confirm.

17.2.3.3.5.4 To export the Authorized URLs list

Context

To keep a copy of the URLs you have authorized for Web Intelligence, you can export them in a JSON file.

You may also use this list to authorize these URLs in the same or another deployment. For more information, see To import a list of Authorized URLs [page 654].

Procedure

1. On the *Central Management Console* home screen, click *Applications*.
2. Select *Web Intelligence*.
3. In the context menu, select *Properties*.
4. Select the *Authorized URLs* section.
5. In the toolbar, click *Export the list of URLs*.

6. Select to export the enabled URLs, disabled URLs or both.
7. Click *Export*.
   A JSON file containing the URLs is generated and saved locally on your file system.

17.2.3.3.5.5 To import a list of Authorized URLs

To quickly authorize URLs, you can import them from a JSON file that lists them. This JSON file must have the following format:

```
[   {  "server": "proxy_server_1",  "port": "proxy_port_1", "url": "URL_1" },
    …
    {  "server": "proxy_server_n",  "port": "proxy_ port_n", "url": "URL_n" },
]
```

where:

- `URL_i` is the authorized URL.
- `proxy_server_i` is the proxy server, if any.
- `proxy_port_i` is the proxy port, if any.

Such file can be generated by exporting an existing list. For more information, see To export the Authorized URLs list [page 653].

Procedure

1. On the *Central Management Console* home screen, click *Applications*.
2. Select *Web Intelligence*.
3. In the context menu, select *Properties*.
4. Select the *Authorized URLs* section.
5. In the toolbar, click *Import a list of URLs to authorize*.
6. Browse on your file system to select a list of JSON files containing the URLs to authorize.
7. Click *Import*.
   The URLs contained in the selected files are added to the list of *Authorized URLs*.

17.2.3.4 Managing Crystal Reports settings

17.2.3.4.1 Enabling Smart View in Crystal Reports

1. Go to the *Applications* area of the CMC and select *Crystal Reports*.
2. Choose *Manage* > *Properties*
   The *Properties* dialog box appears.

3. Choose *BI Launch Pad*.
4. Define the following display option:

Option	Description
Smart View	This option determines which document version is displayed when users open a Crystal Report. • View Latest Instance The latest successful instance of the object is opened. For example, if a document is scheduled for a refresh every hour, and the document was last saved and closed five hours ago, the latest successful instance is opened. • View Object The document is opened in the same state as when it was last saved, irrespective of any scheduled refreshes that might have occurred.

17.2.3.5 Managing alerting settings

In the *Applications* area of the CMC in the BI platform, you can specify system-level settings for alerts.

For the *Alerting* application you can control and define how system users access alerts by:

- Enabling the *My Alerts* folder for alert subscribers
- Enabling and formatting alert messages sent through email
- Setting a limit for the number of alerts in the system
- Setting an expiry period for alert messages

Related Information

Setting user rights on applications [page 626]

17.2.3.5.1 To modify alerting destination properties

Procedure

1. In the *Applications* area of the CMC, double-click *Alerting Application*.
2. Click *Manage* > *Properties*.
   The *Alerting* dialog box appears.

3. (Required) Perform one of the following actions:
   - Select *Enable My Alerts* to enable alert subscribers to receive notifications under *My Alerts* in BI launch pad.
   - Select *Enable Email* to enable alert subscribers to receive notifications through email.
     Global email options for alerts appear.
4. If you selected *Enable Email*, perform the following actions:
   - In the *From* box, enter the email address that alert notifications will be sent from.
     Subscribers will receive alert emails from this email address. Use a valid email address that is recognized by your system.
   - In the *To* box, enter the email address of the alert subscriber.
     By default, all system alerts will be sent to this email address.

     > → Tip
     >
     > Do not specify an email address or recipient. Use the *%SI_EMAIL_ADDRESS%* placeholder.

   - In the *cc* box, enter each recipient email address that should receive carbon copies of alerts.
   - In the *Subject* box, enter a default subject heading to use in emails containing alerts.
   - In the *Message* box, enter a default message to include in emails containing alerts.
   - Select *Add Attachment* to enable attachments to be included by default in emails containing alerts.
     For example, select this option to include associated Crystal reports with triggered alerts.
   - If you selected *Add Attachment*, in the *File Name* select *Automatically Generated* or *Specific Name* to indicate how to name attachments in emails.
5. Click *Save & Close*.

Related Information

Setting user rights on applications [page 626]
Managing alerting settings [page 655]

17.2.3.5.2 To modify Alerting default properties

Procedure

1. Go to the *Applications* area of the CMC and select *Alerting Application*.
2. Click *Manage* > *Properties* > *Default Settings*.
3. Set the appropriate values for the following properties.

Option	Description
Expiry Period	Specifies how long alert messages will be maintained in the system before they are deleted.
Maximum Number of Alert Messages	Specifies the maximum number of alert messages supported by the system. When the threshold is reached, the system will remove 20% of the alert messages, starting with the oldest messages.

4. Click *Save & Close*.

Related Information

Managing alerting settings [page 655]

17.2.3.6 Managing BI Commentary Application Settings

BI Commentary is an application that has been introduced in the CMC. It allows document users to collaborate by commenting on any of the data/statistics available in a given document.

With BI Commentary, users can post comments on data/statistics within the reports.

→ Recommendation

By default, BI Commentary creates and maintains its tables in the Audit database.

> ⓘ Note
>
> To use BI Commentary with the Audit database on a non-windows platform, refer the Data Access Guide to configure ODBC drivers.

However, SAP recommends that you configure a new database to store the comments from BI Commentary application. Databases supported for BI Commentary are the same as those supported for Auditing. The supported databases and corresponding certified jdbc jars for BI Commentary include:

- IBM DB2 Workgroup Edition - db2jcc4.jar
- Microsoft SQL Server - sqljdbc4.jar
- MySQL - com.mysql.jdbc_5.1.5.jar
- Oracle - ojdbc6.jar
- SAP HANA - ngdbc.jar
- Sybase Adaptive Server Enterprise - jconn4.jar
- Sybase SQL Anywhere - jconn4.jar

> ⓘ Note
>
> Irrespective of whether you choose to configure BI Commentary with Audit database or other supported database, for BI Commentary to work with MySQL database, you need to place the MySQL

jdbc jar in the following location: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

If you configure BI Commentary with IBM DB2, you require system temporary table space page size of 8K, 16K, or 32K. By default, the page size is 4K.

> **Note**
>
> If the Audit database is not configured/enabled by default, then BI Commentary does not work unless you manually configure a new database for BI Commentary.
>
> If you configure BI Commentary with Audit Database, and you delete the Audit Database, all comments stored in the Audit Database are also deleted.
>
> The Audit database uses either ODBC or native database driver types. To configure a new Commentary database, you require a JDBC driver.

> **Note**
>
> Size of a comment is limited to 2000 UTF-8 character bytes or 666 UTF-16 character bytes.

> **Note**
>
> You cannot migrate comments using Federation Tool.

> **Note**
>
> BI Commentary is not supported for MaxDB connections.

> **Note**
>
> To delete commentary entries made by user, use the following query:
>
> `DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'`

17.2.3.6.1 Configuring a New BI Commentary Database

Prerequisites

You have created a JDBC connection.

> **Note**
>
> When you configure a new BI Commentary database, the Commentary Service housed in the Adaptive Processing Server is responsible for writing Commentary information to the database. The following steps should be taken on every machine in the cluster where the Commentary Service is running.

To create a new JDBC connection, perform the following:

1. Place the JDBC driver jar for the database that you want to configure in the following location: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

   > **Note**
   >
   > If you upgrade to SAP BusinessObjects Business Intelligence Platform 4.2 Support Package 2, and had already configured a new database for BI Commentary from the earlier versions, you need move the database driver file from the 'jdbc' folder in `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\external>` to `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

2. Restart SIA.

Context

To configure a new database for BI Commentary, proceed as follows:

Procedure

1. Log on to the CMC.
2. From the CMC Home page, select *Applications* from the dropdown menu.
3. In the *Application Name* list, choose *BI Commentary Application*.

   The *BI Commentary* popup window appears. By default, the *Use Audit Database* radio button is selected.
4. Select the *Use other supported database* radio button.
5. Enter the *Type*, *Database Name*, *Host*, *Port*, *User Name*, and *Password* in the *Configure Commentary Database* pane.
6. Choose *Save & Close*.
7. Restart APS.

   Any changes to the configuration of BI Commentary database will only take into effect after you restart the Adaptive Processing Server (APS).

   You may validate your connection by choosing *Test Connection*.

   > **Note**
   >
   > If you upgrade to SAP BusinessObjects Business Intelligence Platform 4.3 Support Package 3 and had already configured a database for BI Commentary for JDBC from the earlier versions, the password field will now become blank when selecting *Test Connection*, *Save & Close*, or *Save*.

   You may choose to delete or clean up older comments by checking the *Delete all comments older than* checkbox, and specifying the number of days.

> **Note**
>
> You need to restart all APS servers that host BI Commentary service for the changes to take effect.

Results

You have now configured a new database to store comments from the BI Commentary application.

17.2.3.7 Managing BI Admin studio Application settings

> **Note**
>
> To Access BI Admin Studio, you should be a part of the Administrator group.

If you deny specific access rights such as: *Allow access to BI Admin Cockpit*, *Allow access to Monitoring*, and *Allow access to Visual Difference*, you might not be able to access the specific application in BI Admin Studio.

Specific Rights for BI Admin Studio	Implicit Value
Allow access to BI Admin Cockpit	Granted
Allow access to Monitoring	Granted
Allow access to Visual Difference	Granted
Visual Difference - Create comparison	Granted
Visual Difference - Delete comparison	Granted
Visual Difference - Rerun comparison	Granted
Visual Difference - View comparison	Granted

If the *Visual Difference* rights are denied, then you can also restrict the VD application usage.

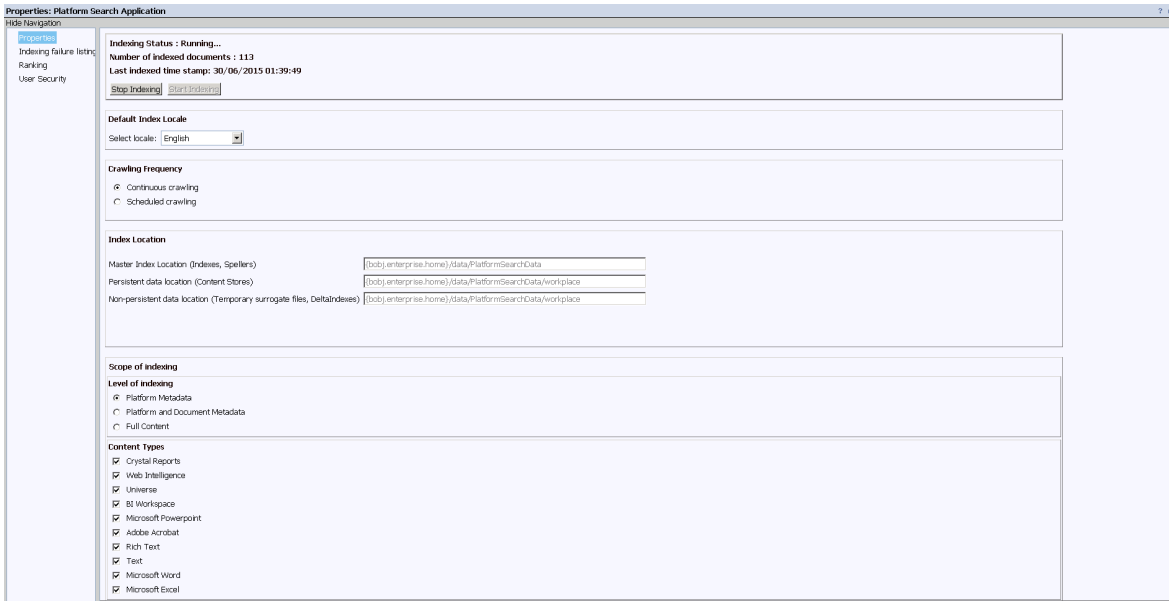
17.2.3.8 Managing Platform Search settings

In the *Applications* area of the CMC in the BI platform, you can specify system-level settings for the Platform Search application.

17.2.3.8.1 Configuring Application Properties in the CMC

To configure the Platform Search application properties, complete the following steps:

1. Go to the *Applications* area of the CMC.
2. Select *Platform Search Application*.
3. Click *Manage* > *Properties*. The *Platform Search Application Properties* dialog box appears.



4. Configure the Platform Search settings:

Option	Description
Search Statistics	Platform Search offers the following search statistics: • Indexing Status: displays the status of the indexing process. • Number of indexed documents: displays the number of documents that are indexed. • Last indexed time stamp: displays the time stamp at which the document was last indexed.
Stop / Start Indexing	Start or Stop Indexing options enable you to start or stop the indexing process when you want to switch from continuous crawling to scheduled crawling, or for maintenance purposes. To stop indexing, click *Stop Indexing*.
Default Index Locale	Platform Search uses the locale specified in the CMC for indexing all the non-localized BI documents. Once the document is localized the corresponding language analyzer is used for indexing. Search is based on the client's product locale, and the weighting is given to the client's product locale. You can configure the weighting in the CMC configuration properties.

Option	Description
Crawling Frequency	You can index the entire BI platform repository by using the following options: • Continuous crawling: With this option, indexing is continuous; the repository is indexed whenever an object is added, modified, or deleted. It allows you to view or work with the most up-to-date BI platform content. Set by default, continuous crawling updates the repository continuously with the actions that you perform. Continuous crawling works without user intervention, and reduces the time taken for indexing a document. • Scheduled crawling: With this option, indexing is based on the schedule set by the Schedule options. For more information about scheduling an object, refer to the *Scheduling an Object* section of Platform Search in the *SAP BusinessObjects Business Intelligence platform CMC Online Help*. **Note** • If you select *Scheduled Crawling* and set the *Recurrence* to an option other than *Now*, Platform Search displays the date and time stamp when the document is scheduled to be indexed next. • If you select *Scheduled Crawling*, then the *Start Indexing* button is enabled and the *Stop Indexing* button is disabled. • Once the scheduling is complete, the *Stop Indexing* button is disabled.

Option	Description
Index Location	The indexes are stored in shared folders in the following locations: • Master index location (indexes and speller): The master and speller indexes are stored in this location. During a search, the initial results are retrieved using the Master Index, and the speller indexes are used to retrieve suggestions. In a clustered BI platform deployment, this location should be on a shared file system that is accessible from all nodes in the cluster. • Persistent data location (Content stores): The content store is placed in this location. It is created from the master index location and remains synchronized with it. The content store is used to generate facets and process the initial hits generated from the Master Index location. In a clustered BI platform deployment, content stores are generated at every node. The persistent data location is the only index location that is affected by the clustered environment as it contains the content store folders. If a machine has a single search service, then there will be only one content store location. For example, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. However, in a clustered environment, if there are multiple search services, then each search service will have one content store location. For example, if you have two instances of a server running, then the content store locations would be as follows: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name 1>\ContentStores. • Non-persistent data location (Temporary files, Delta Indexes): In this location, the delta indexes are created and stored temporarily before being merged with the Master index. The indexes at this location are deleted once they are merged with the Master Index. In addition, surrogate files (output of the extractors) are created in this location and stored temporarily until they are converted into delta indexes. **Note** • Master index location must be a shared location. • You need to click *Stop Indexing* to modify the index location. • If you modify an index location, copy the content to a new location, or the existing index information will be lost. • The index files might store personal and confidential information, especially when you choose to index document content. You must allow only a system user to access the shared folder and you should store the shared folders in an encrypted environment to avoid data theft.

Option	Description

Level of indexing	You can tune the search content by setting the level of indexing in the following ways:
	• Platform Metadata: An index is created only for the platform metadata information such as titles, keywords, and descriptions of the documents. By default, this option is selected.
	• Platform and Document Metadata: This index includes the platform metadata as well as the document metadata. The document metadata includes the creation date, modification date, and name of the author.
	• Full Content: This index includes the platform metadata, document metadata, and other content such as:
	  • The actual content in the document
	  • The content of prompts and LOVs
	  • Charts, graphs, and labels
	Note
	Full content indexing is not supported for Analysis Office and Lumira documents. Only metadata indexing is supported for Analysis Office and Lumira documents.
	Note
	When you modify the level of indexing, the indexing is initialized for the entire BI platform repository refresh.

Content Types	You can select the following content types for indexing: • Crystal Reports • Web Intelligence • Universe • BI Workspace • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Rich Text • Text • Microsoft Word • Microsoft Excel The content type filter does not apply for platform metadata indexing. Regardless of the content types you select, platform metadata indexing happens for all the supported object types and the search results in BI launch pad returns all the objects for the keyword related to platform metadata. The content type filter is relevant for document metadata indexing (document author, document header, document footer, and so on) and content indexing (graphs , charts , table with a report). Based on the level of indexing and content types you select, platform search indexes the document metadata and content for the selected objects types from the repository and only those objects appear in the BI launch pad search results, when searching for keyword related to document metadata and content.

Option	Description
Rebuild index	This option deletes the existing index and re-indexes the entire repository. You can select the *Rebuild index* option whether indexing is running or stopped. The existing index is deleted when you save your changes to the properties page. However, if indexing is currently stopped, the index does not start rebuilding until you restart indexing. If you do not want Platform Search to re-index the documents, clear the *Rebuild index* option before clicking *Start Indexing*.
Documents Excluded from Indexing	The *Documents Excluded from Indexing* option excludes documents from indexing. For example, you may not want extremely large Crystal reports to be made searchable to ensure the report application server resources are not overloaded. Similarly, you may not want publications with hundreds of personalized reports to be indexed. By excluding particular documents, you can prevent them from being accessed by Platform Search. It is important to note that if a document is already indexed before it is put into this group, the document may still be searchable. To ensure that documents in the *Documents Excluded from Indexing* group are not searchable, you must rebuild the index. By default, only the Administrator account has full control of the *Documents Excluded from Indexing* option. Other users with the following rights can only add documents to the *Documents Excluded from Indexing* group: • View and edit rights on the category • Edit the document directly
Other Configuration - Skip Instance	By default, instances of documents are picked for indexing. This causes inflated index size resulting in more consumption of disk space. The size of "Lucene Index Engine" folder within PlatformSearchData folder grows huge due to indexing of huge number of instances in the repository. If there are millions of documents (or more) and many of these documents also have huge number of existing instances (along with scheduled instances generated in regular interval) in the system, then the size of "Lucene Index Engine" folder grows excessively even if the indexing level is set to "Platform Metadata". Platform Search Skip Instance feature allows you to control the indexing of instances by enabling or disabling, through check box under 'Other Configuration - Skip Instance' in Platform Search Application properties page in CMC. **Note** • If you Enable/Disable Skip Instance, you need to restart Platform Search Adaptive Processing Server. This change affects all levels of indexing. • If you modify Skip Instance and want the changes to be applied to all existing instances (i.e. to be picked for indexing), then you need to rebuild index.

Option	Description
Objects Excluded from Indexing	The *Objects Excluded from Indexing* option excludes objects from indexing. For example, you may not want certain objects to be made searchable to ensure the report application server resources are not overloaded. By excluding particular objects, you can prevent them from being accessed by Platform Search. It is important to note that if an object is already indexed before it is put into this group, the object may still be searchable. To ensure that documents in the *Objects Excluded from Indexing* group are not searchable, you must rebuild the index. List of objects that can be excluded from indexing: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • Rtf • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • Profile • Event • Discussions • InformationDesigner • MDAnalysis • Publication • Agnostic • Analytic • Hyperlink • Program • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset • VISI.Lums

Option	Description
	• VISILums • User • UserGroup

5. Click *Save & Close*.

> **Note**
>
> If a user does not select the *Rebuild Index* option and changes the level of indexing or selects or deselects extractors, then the index is incrementally updated without deleting the existing index.

17.2.3.9 Configuring SAP HANA single sign-on

In the *Applications* area of the CMC in the BI platform, you can configure single sign-on (SSO) for SAP HANA database connections. SSO is implemented using SAML (Security Assertion Markup Language).

Once you have established a BI platform session, you will be able to generate a SAML ticket that can be used to log in to SAP HANA without requiring the user to provide a password.

This is the basic workflow involved in connecting to SAP HANA data sources:

1. An administrator configures a trust between SAP HANA and the BI platform in the CMC.
2. A user logs into the BI platform with any of the supported authentication providers.
3. Provided that the SAP HANA and BI platform user IDs match, the BI platform is able to generate a SAML assertion that SAP HANA can accept to establish a connection for the current user. The user ID that is passed to SAP HANA is the BI platform user ID for the user that logged in.
4. A BI platform client application creates an SAP HANA connection.

> **Note**
>
> Before configuring SAP HANA single sign-on with SAML, you must configure SSL on the SAP HANA machine. See your SAP HANA documentation for details.

17.2.3.9.1 SAP HANA connection settings

The table below summarizes the settings available in the CMC for configuring SAP HANA connections.

Setting	Description
HANA Hostname	Provide the name of your SAP HANA host.
HANA Port	Provide the port number for your SAP HANA host.
Unique Identity Provider ID	A unique name within a given HANA installation. The HANA installation will accept properly signed tickets from this identity provider name for logons.

Setting	Description
Identity Provider Base64 Certificate	When you click *Generate*, a certificate is created in the *Identity Provider Base64 Certificate* field. Copy this certificate to the `trust.pem` file in your SAP HANA deployment. This certificate establishes the trust relationship between SAP HANA and the BI platform. The external identity provider itself is identified with an X509 certificate, which is used to sign all identity assertions. The certificate must be Base64 encoded.
HANA Instance Number	Provide the instance number of your SAP HANA database.
HANA Tenant Database	Provide the name of your SAP HANA tenant database.

17.2.3.9.2 To create an SAP HANA connection

Procedure

1. Get the relevant SAP HANA database parameters.
   a. Open the SAP HANA Studio application.
   b. Open the properties page for your system, and find the URL for the database connection.
   c. Record the host machine name, the port number, instance number, and tenant database name.

      You'll need this information in step 2.
2. Configure an SAP HANA connection in the BI platform.
   a. Go to the *Applications* area of the CMC and double-click *HANA Authentication*.
   b. In the *HANA Authentication* dialog box, click the *Create a connection* button.
      The *Create HANA Authentication Connection* dialog box opens.
   c. Choose a *Connection Type*.

      > **Note**
      >
      > You should choose *SAP HANA* for a JDBC connection and *SAP HANA HTTP* for an HTTP connection.

   d. Enter the port number, host machine name, instance number, and tenant database name that you had recorded in step 1.
   e. In the *Unique Identity Provider ID* field, specify a value that will be used for your BI platform deployment.
   f. Enter *Service Provider Name*.

      > **Note**
      >
      > You can check the configuration of Service Provider Name in HANA by navigating to `indexserver.ini -> Authentication -> saml_service_provider_name`. You can also change the value in HANA by entering the code mentioned below: `ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') SET ('authentication', 'saml_service_provider_name') = 'DEV00' WITH RECONFIGURE;` In the code, DEV 00 is the name of service provider and you can enter it as per your choice. The best practice to name the service provider is to combine System ID (DEV) and Instance number (00).

g. Select *Secure Connection*.

> **Note**
>
> You must select *Secure Connection* to establish a secure JDBC or HTTPS connection.
>
> - To establish an HTTPS connection, you must choose *SAP HANA HTTP* as the *Connection Type* and select *Secure Connection*.
> - To establish a secure JDBC connection, you must choose *SAP HANA* as the *Connection Type* and select *Secure Connection*.

h. Click *Generate*.
A certificate is created in the *Identity Provider Base64 Certificate* box.

3. Configure your SAP HANA deployment.
   a. Login to the HANA system.
   b. Expand *SSL and Trust Configuration* and select *PSE Management*.
   c. Select the PSE file from the dropdown against *Manage PSE*.
   d. Select *Import Certificates*.
   e. Paste the certificate generated in the earlier step in the BI platform.
   f. Select *Import*
   g. Launch SAP HANA Studio.
   h. In the *Systems* view, expand your SAP HANA system. Refer to SAP HANA One Administration Guide.
   i. Open (Security Editor) from the Security folder.
   j. Select (Import SAML Identity Provider for Certificate File).
   k. Choose your identity provider from the *SAML Identity providers* list.
   l. Select (deploy).
   m. Navigate to the HANA user in the *Systems* view.
   n. Open the HANA user in the Editors area.
   o. In the *User* tab, check *SAML* as the authentication and select *Configure*.
   p. In the *Configure External SAML Identities* wizard, select *Add*.
   q. Select your identity provider.
   r. Select OK.
   s. Select your identity provider and enter the BI platform user's name that is mapped to the HANA user against it.
   t. Select OK.
   u. Select (deploy).
   v. Restart the SAP HANA System.
      1. Open the context menu of your SAP HANA system.
      2. Select *Configuration and Monitoring*.
      3. Choose *Restart System*.
4. Test the SAP HANA configuration.
   a. Go to the *Applications* area of the CMC and double-click *HANA Authentication*.
   b. In the *HANA Authentication* dialog box, open the connection you created in step 2.
   The *Edit HANA Authentication Connection* dialog box opens.
   c. Under *Test the connection for this user*, enter a user name and click the *Test Connection* button to verify that your connection settings are valid.

For example, enter the user name `Administrator`. If the settings are not valid, an error message is displayed. You can try these troubleshooting steps:

- Ensure that no other certificate in the `trust.pem` file contains a Subject or Issuer with the same CN property value. To see the components of the certificate, search the internet for "x509 certificate decoder" to find a certificate decoder.
- Try these commands to check the HANA-side configuration:

```
select * from "SAML_PROVIDERS"
select user_name, is_saml_enabled from users where user_name =
'<UserName>'
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

- If a SAML authentication error is displayed while configuring SSO to SAP HANA, try these steps:
  1. In the `indexserver.ini` file, set the parameter `sslCreateSelfSignedCertificate` to `false`.
  2. In the same file, set the parameters `sslKeyStore` and `sslTrustStore` to use absolute paths.
  3. Regenerate the `key.pem` and `trust.pem` files.

Results

If the `key.pem` file does not exist in the `.ssl` directory, then SAP HANA was not configured correctly to use SSL.

17.2.3.9.3 Configuring SAP HANA HTTPS Connection

The configuration of SAP HANA HTTPS includes adding the HANA server and HANA server CA certificate in TrustStore or any location of your choice.

> **Note**
>
> You must export the SAP HANA Server certificate from the SAP HANA system before adding the certificate to the TrustStore or in a different location.

Adding the Certificate in TrustStore

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
2. Run the command: `..\..\bin\keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.
3. The HANA server and HANA server CA certificate are stored in the TrustStore.

> **Note**
>
> If the keystore file is located at the default location `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`, the changes made to the keystore file

is lost after an upgrade from SAP Business Intelligence Platform Support Package 4 to Support Package 5. Hence, it is recommended to add the certificate in a different location.

Adding the Certificate in Different Location

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Run the command: `keytool -importcert -file "C:\certificate\HANASERVERCertificate " -alias CertificateAliasName -keystore C:\certificate\cacerts -storepass changeit`.

   > **Note**
   >
   > The location defined above is just an example. You can add any location of your choice.

3. For the APS server to identify the file location, run the command:

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **Note**
   >
   > cacerts_PATH and Password are just examples of the keystore path and certificate password. You can add any path and password of your choice.

17.2.3.10 Managing SAP Lumira Settings

From the "Applications" area of CMC, you can manage rights related to data acquisition and content sharing functionality of SAP Lumira for each user or user group.

To manage rights for SAP Lumira, perform the following steps:

1. From the CMC Home page, select *Applications* > *SAP Lumira* > *User Security*.
2. Select the user or group you want to set rights for.
3. Select *Assign security*.
4. Select *Advanced*.
5. Select *Add/Remove rights*.
6. Define the rights that the user needs to have for SAP Lumira.
7. Click *Apply*.

17.2.3.11 Authorization Server Configuration

The Authorization Server Configuration application is for any database resources to access through the Authorization Server mechanism or protocol.

End to End SSO OAuth Support - Single and Multiple OAuth Server Support

In the Central Management Console, the *Authorization Server Configuration* application allows you to configure and manage authorization servers in the BI Platform. Within the application, the administrator is responsible for registering and managing the configurations via the authorization reference objects. Each authorization server configuration has an authorization reference object. You can create authorization server configurations for agnostic, Google Drive, Microsoft Drive, or OData resources.

To create an authorization server configuration, fill in the mandatory fields under *Enter Configuration Information for an Authorization Server*.

The *Authorization Scope* can be defined based on your needs to help control what end users have access to, whether online or offline.

17.2.3.11.1 To configure an authorization server

You can configure an authorization server.

Procedure

1. Launch and log in to the Central Management Console as an Administrator.
2. In the home page, select *Applications* under the *Manage* column.
3. In the *Applications* page, double click on *Authorization Server Configuration*.
4. In the *Authorization Server Configurations* dialog, do one of the following:
   - Select *Manage* > *New Authorization Server Configuration*
   - Select the *Create a New Authorization Server Configuration* toolbar icon
5. Fill in the following parameters in the *Create a New Authorization Server Configuration* dialog:
   - *Reference Name*
     Choose a unique random string and enter the same to identify the configuration, to recognize and choose the configuration in different workflows for achieving authorization based SSO.
   - *Description* (optional)
     Enter any statement or keyword to describe and easily identify the configuration out of the list of available configurations.
   - *Grant Type*

Choose the desired method for authorization grant type out of the available list of supported grant types by the BI Platform. The following is the current list of grant types which are supported in the BI Platform to select based on your client application settings at the authorization server:

- **Authorization Code** (default value)
  - If your client application at authorization server, of which you are going to enter the client id and client secret is configured to allow the access by an end user authorization by validating the authorization code grant, then choose this option.
- **Client Credentials**
  - If your client application at authorization server, of which you are going to enter the client id and client secret is configured to allow the access by the client credential flow without any end user authorization, then choose this option.

> **Note**
>
> Since this parameter is newly introduced, if you are updating your system from a previous version where the **Grant** Type parameter did not exist and already have **Authorization configurations** in place, the update will automatically set the grant type value to **Authorization Code** as the default for those existing configurations.

- **Fields specific to OpenID Connect**
  The following fields are specific to OpenID Connect authentication, and they are not required for authorization SSO:
  - *Enabled for "OpenID Connect" Authentication* check-box
  - *Issuer URI*
  - *JSON Web Key Sets URI (jwks_uri)*
  - *ID Token Signing Algorithm*
- *Authorization Endpoint*
  Enter the URL of the authorization server, with which you can get the authorization grant.
- *Token Endpoint*
  Enter the URL of the authorization server, with which you can request an access token by exchanging the authorization code.
- *Client ID*
  Enter the name of the application, which is used to register the BI landscape with the authorization server.
- *Client Secret*
  Enter the specific secret code corresponding to the application which is used in registering the BI landscape with authorization server.
- *Redirect URL*
  Enter the URL of the BI landscape endpoint to which the authorization code must be sent by the authorization server after the successful validation of the authorization.
- *Revocation Endpoint* (optional)
  Enter the URL of the authorization server, with which application can request the revocation of all previously issued access tokens through a specific refresh token.
- *Authorization Scope*
  Enter the supported authorization scopes by the authorization server to define the limits for the application (BI landscape) access to different API resources available.

> **Note**
>
> BI Platform implementation of OAuth SSO is based on offline access. If your aim for configuration the authorization server in BI Platform is to refresh data or access resources without being challenged for the authorization validation every time, then you need to configure this field with required scope parameter along with one mandatory parameter (for example, either "refresh_token" or "offline_access" based on the vendor of the authorization server.

- *Type of Resource*
  Choose the desired resource type out of the available list of supported resource types by the BI Platform. The following is the current list of resource types which are supported in the BI Platform to configure and access through the corresponding authorization server:
  - *Agnostic* (default value)
    Not specific to any vendor or protocol, to indicate any resource which can be accessed with a successful authorization grant by an authorization server.
  - *GoogleDrive*
    To indicate that the configuration is of Google authorization server which can be used for accessing Google Drive to different BI Platform scenarios. At any point of time, only one configuration of type GoogleDrive can exist in the system.
  - *Microsoft Drive*
    To indicate that the configuration is of Microsoft authorization server which can be used for accessing Microsoft Drive to different BI Platform scenarios. At any point of time, only one configuration of type Microsoft Drive can exist in the system.
  - *OData*
    Not specific to any vendor, but to indicate that the configuration is related to a resource which can be accessed through the OData protocol with an authorization grant by an authorization server. Like GoogleDrive, at any point of time only one configuration of type OData can exist in the system.

> **Note**
>
> The *Type of Resource* parameter has nothing to do with the OAuth 2.0 standard. However, this is introduced in the configuration to avoid any possible ambiguity in identifying certain resources in the BI Platform. Therefore, the corresponding configurations can be easily picked and used in certain scenarios to achieve authorization.

- *Access Type*
  This parameter is specific to the authorization configuration of type *GoogleDrive*. It will be auto-filled when the value for the *Type of Resource* field is *GoogleDrive*.
- *Custom Parameters* (optional)
  Enter any custom parameters required to send while requesting the authorization. This is based on any custom requirements (if required) of the authorization server being configured.

> **Note**
>
> The name of the custom parameter should be unique in the configuration.
>
> In any authorization configuration, there is a maximum of five custom parameters allowed to be configured.

6. Click on *Test Connection* to test the configuration.
   Wait for the configuration test result in a popup window.

- If the result is not successful close the popup window, cross check and update the input values for the configuration parameters. And click on *Test Connection* button again.
- Repeat the above step, until you see a successful result for the connection, and close the popup window.

7. Re-enter the *Client Secret* before clicking *OK* or after each Test Connection, as it is cleared for security reasons.

> **Note**
>
> The "Client Secret" field must be re-entered just before clicking the "OK" button each time you create or edit the configuration. After clicking the "Test Connection" button, the "Client Secret" value will be cleared for security reasons. Therefore, after each test (successful or not), you must enter the correct "Client Secret" to proceed with the next iteration of the test or to save the configuration. This ensures the "Client Secret" is not fetched from the backend due to security standards

8. After filling all the required parameters, select *OK* to validate the details and save the configuration.

   The configuration will be saved as a system object in the repository with type *AuthorizationReference*. You can refer to the configuration in all supported scenarios with its *Reference Name*.

17.3 Managing applications through Semantic Layer Properties

Dimensional Semantic Layer (DSL) library configuration options may be set at runtime to change the behavior of HANA Direct Access, and BW Direct Access via BICS connections in BI tools such as Web Intelligence, and Information Design Tool. These options are specified via Java command-line options of the form:

-DoptionName=optionValue

Maintaining and modifying these settings may pose challenges:

- The command-line options must be specified for each and every Java process running DSL. There is no common location to make changes.
- Each and every DSL Java process must be restarted for revised settings to take effect. Changes do not take effect on-the-fly.

To simplify the administrative task of maintaining DSL-BICS configuration options, a new mechanism is introduced, where the options may be stored in a file. Changes to the file will propagate the new option settings to all DSL processes that read the file.

The option name and value are stored on file as valid XML for java.util.Propertes as defined by http://java.sun.com/dtd/properties.dtd

When you first initiate this new mechanism by running DSL, the following two files are automatically generated:

- DSLBICSConfiguration.xml or DSLConfiguration.xml - this file contains all available options and their default values. This file should not be modified.
- DSLBICSConfiguration_custom.xml or DSLConfiguration_custom.xml - this file contains all options with administrator specified values.

> **Note**
>
> - DSLBICSConfiguration.xml and DSLBICSConfiguration_custom.xml files are used to manage the behavior of BW Direct Access via BICS connections.
> - DSLConfiguration.xml and DSLconfiguration_custom.xml files are used to manage the behavior of HANA Direct Access.

The generated `DSLBICSConfiguration_custom.xml` and `DSLConfiguration_custom.xml` file contains all option settings specified via command-line and default settings for other options. Subsequent to its initial generation, the `DSLBICSConfiguration_custom.xml` or `DSLConfiguration.xml` file may be modified to add or alter option values. The mechanism does not update this file subsequent to its initial generation. The mechanism updates the `DSLBICSConfiguration.xml` file with new available options, or if there is an evolution for a default value.

To modify any of the default properties, use the custom configuration file to save new settings for either global or application-specific properties. By default, the directory files is are located at: `SAP BusinessObjects Enterprise XI 4.0\java\lib`

Do not modify the properties in the default configuration file.

17.4 Managing applications through BOE.war properties

17.4.1 The BOE war file

You can modify settings for BI platform web applications by overwriting default properties for the BOE.war file. This file is deployed on the machine hosting the web application server. For detailed information on how the file is deployed see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide.*

The properties contained in the BOE.war file control specifications for default login behavior, default authentication methods, settings for single sign-on. There two types of properties you can specify:

- Global properties - these properties affect all the web applications contained in the BOE.war file.
- Application-specific properties - property settings that affect only a specific web application.

To modify any of the default properties, use the custom configuration directory to save new settings for either global or application-specific properties. By default, the directory is located at: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Do not modify the properties in the `config\default` directory.

> **Note**
>
> On some web application servers such as the Tomcat version bundled with the BI platform, you can access the BOE.war directly. In this scenario, you can set custom settings directly without undeploying the WAR file. When you cannot directly access the deployed web applications, you must undeploy, customize, and then redeploy the file. For more information, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide.*

17.4.1.1 Global BOE.war properties

The following table lists the settings included in the default `global.properties` file for BOE.war.

To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Default values	Description
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Enables or disables persistent cookies on the web application logon page.
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Specifies what authentication method to use with SiteMinder. Only options are secLDAP and secwinAD.
`siteminder.enabled`	`siteminder.enabled=false`	Enables and disables authentication with SiteMinder.
`sso.enabled`	`sso.enabled=false`	Enables and disables single sign-on (SSO) to BI platform.
`sso.sap.primary`	`sso.sap.primary=false`	Set to `true` if you want to use SAP SSO as the application's primary single sign-on mechanism. Only applies to cases where both SAP and SiteMinder SSO are used.
`max.tree.children.threshold`	`max.tree.children.threshold=200`	Specifies the threshold at which the tree list control will not display all the nodes, and will instead display a "too many children" message.
`trusted.auth.shared.secret`	None	Specifies the session variable name used to retrieve the secret for Trusted Authentication. Only applies if using the web session to pass the shared secret.
`trusted.auth.user.param`	None	Specifies the variable used to retrieve the user name for Trusted Authentication, and can be set to one of the following values: • `Header` • `URL Parameter` • `Cookie` • `Session`
`trusted.auth.user.retrieval`	None	Specifies the method used to retrieve the username for Trusted Authentication., and can be set to one of the following values: • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"` • `"USER_PRINCIPAL"` Set to empty to disable Trusted Authentication.

Setting	Default values	Description
`trusted.auth.user.namespace.enabled`	`trusted.auth.user.namespace.enabled=false`	Enables and disables dynamic binding of aliases to existing user accounts. If property is set to `true`, Trusted authentication uses alias binding to authenticate users to the BI platform. With alias binding, your application server can work as a SAML service provider therefore enabling Trusted Authentication to provide SAML SSO to the system. If set to `false`, Trusted Authentication uses name matching to authenticate users.

`vintela.enabled`	`vintela.enabled=false`
	`idm.realm=YOUR_REALM`
	`idm.princ=YOUR_PRINCIPAL`
	`idm.allowUnsecured=true`
	`idm.allowNTLM=false`
	`idm.logger.name=simple`
	`idm.logger.props=error-log.properties`
		Used to enable or disable Vintela settings for Windows AD authentication.

`pinger.showWarningDialog.cmc`	`pinger.showWarningDialog.cmc=true`	Specifies whether or not to display the warning dialog with the message indicating that the current session will expire soon in the CMC.
`pinger.showWarningDialog.bilaunchpad`	`pinger.showWarningDialog.bilaunchpad=true`	Specifies whether or not to display the warning dialog with the message indicating that the current session will expire soon in BI launch pad.
`pinger.warningPeriod.pingIncrementsInSeconds`	`pinger.warningPeriod.pingIncrementsInSeconds=15`	Specifies how often a web server request should be sent while the session expiry warning message is displayed. This is important for synchronizing the warning dialog across applications.
`pinger.warningPeriod.lengthInMinutes`	`pinger.warningPeriod.lengthInMinutes=5`	Specifies how long prior to session expiry the warning should be displayed.
`logoff.on.websession.expiry`	`logoff.on.websession.expiry=true`	Specifies if all application sessions log off when the web session expires.
`pinger.enabled`	`pinger.enabled=true`	Enables or disables the session expiry warning messaging mechanism.
`system.com.sap.bip.jcomanager.destinations.maxsize`	`system.com.sap.bip.jcomanager.destinations.maxsize=1000`	Specifies the maximum number of cached Java connections.
`httpproxy.username`	`httpproxy.username=myusername`	Specifices the username to log on to the HTTP proxy server.
`httpproxy.password`	`httpproxy.password=mypassword`	Specifices the password to log on to the HTTP proxy server.
`logon.embed.secret`	None	A shared secret between a portal that embeds BI platform applications and the BI platform application server, which is used to determine

Setting	Default values	Description
		whether BI platform applications can be safely embedded in other pages.
`logon.embed.timeout`	`logon.embed.timeout=300`	The number of seconds after which BI platform applications such as BI launch pad will reject being embedded into a portal. Ensure that the system clocks on the BI platform web server and the portal server machines are within this number of seconds of each other.
`pinger.showWarningDialog`	`pinger.showWarningDialog=true`	Specifies whether or not to display the warning dialog with the message indicating that the current session will expire soon. Does not apply to the CMC & BI launch pad.
`ure.request.queue.timeout.seconds`	`ure.request.queue.timeout.seconds=20`	The number of seconds a request will wait for expected previous requests before timing out When users perform navigation or folder expansion actions in the tree list control in the BI launch pad, AJAX requests are queued for those actions. The user interface waits for these requests to complete before relinquishing control to the user. This setting determines the number of seconds that the user interface will wait for each request, if unexpected delays occur in the back-end query.
`enable.safe.html`	`enable.safe.html=true`	Enables usage of safe web page URLs in the web page module URLs for BI Workspace.
`upload.file.maxsize.in MB`	`upload.file.maxsize.in MB = 0`	Specifies the maximum file size for uploading files in Megabytes. When default value i.e 0 is set, files of any size can be uploaded.
`upload.file.allowed.formats`	None	Specifies the allowed file formats for uploading files. For more information, see 2296060.
`upload.file.maxsize.in MB=0`	None	Maximum file size for Local Document upload in MegaBytes and it should be whole number E.g: 10 etc.
`upload.file.allowed.formats=`	None	This property is used to control different file types allowed for uploading Local document. refer the SAP Note 2296060 for getting supported file format list. If your defining multiple formats separate each file format followed by comma such as txt,doc,xls.

Setting	Default values	Description
`offlinehelp.enabled=false`	None	Set offlineHelp flag to true to enable the offline help. By default, this value is set to false.
`offlinehelp.url=`	None	The offlinehelp.url will be consumed while user has set the offline flag to true
`SMTPFrom`	None	Enables or disables the From field in Central Management Console (CMC) when scheduling an object to a destination. Default: `SMTPFrom=true`. When the value is set to false the From field will not be displayed in Central Management Console (CMC) and the system attempts to retrieve the From email value in the following order: 1. First, from the report default for a report object. 2. Second, from the email address on the user profile of the logged on user. 3. Lastly, from the Job server default.

17.4.1.2 BI launch pad properties

The following table lists the settings included in the default `bilaunchpad.properties` file for the BOE war file. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Description
`app.name`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name=BI launch pad`
`app.name.short`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name.short=BI launch pad`
`app.url.name`	Specifies the URL name of the application, preceded by the "/"" character. Default: `app.url.name=/BI`
`authentication.default`	Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting: **Authentication** / **Setting value** Enterprise / `secEnterprise` LDAP / `secLDAP` Windows AD / `secWinAD`

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td></td><td><table>
<tr><th>Authentication</th><th>Setting value</th></tr>
<tr><td>SAP</td><td>secSAPR3</td></tr>
<tr><td>PeopleSoft</td><td>secpsenterprise</td></tr>
</table>
Default:
authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Specifies if users logging into BI launch pad have the option to view and change the authentication method. Default: authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>Specifies the visibility of the list of available authentication types in the login screen. Following is the list of available authentication types: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise. From among the list, you can choose to enable or disbale authentication types by either including or excluding the desired authentication types from the Authentication.VisibleList. Default: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise</td></tr>
<tr><td>sap.system.client.visible
authentication.sapSystem
authentication.sapClient</td><td>Specifies the visibility of the SAP System and SAP Client fields, when you select the authentication type as 'SAP'. Default: sap.system.client.visible=true. When sap.system.client.visible is set to sap.system.client.visible=false, you can specify the values for SAP System and SAP Client in the properties file by using authentication.sapSystem and authentication.sapClient parameters respectively.</td></tr>
<tr><td>cms.default</td><td>Specifies the default CMS name. Default: cms.default=[name of host machine]</td></tr>
<tr><td>cms.visible</td><td>Specifies if users logging into BI launch pad have the option to view and change the CMS name. Default: cms.visible=true</td></tr>
<tr><td>dialogue.prompt.enabled</td><td>Specifies if users should be prompted when navigating away from an input page in a dialog box. Default: dialogue.prompt.enabled=false</td></tr>
<tr><td>logontoken.enabled</td><td>Specifies whether or not to enable token creation for the session after a user logs into BI launch pad. Token will be stored in a cookie. Default: logontoken.enabled=false</td></tr>
<tr><td>SMTPFrom</td><td>Enables or disables the From field when scheduling an object to a destination. Default: SMTPFrom=true</td></tr>
</table>

Setting	Description
	When the value is set to `false` the *From* field will not be displayed and the system attempts to retrieve the *From* email value in the following order: 1. First, from the report default for a report object. 2. Second, from the email address on the user profile of the logged on user. 3. Lastly, from the Job server default.
`url.exit`	Specifies which URL to redirect users after terminating their BI launch pad session. This setting applies only to users who have logged into the application through an external verification process.
`disable.locale.preference`	Enables or disables the user from viewing and thus modifying the viewing local preferences for BI launch pad. Default: `disable.locale.preference=false`
`extlogon.allow.logoff`	Enables or disables automatically logging off user sessions once they have closed their BI launch pad session. Set to false if you want user sessions not to automatically terminate when users log off BI launch pad. Default: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Specifies whether to allow other pages to embed this application (as a frame) without passing a valid embed token. Default: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Specifies a comma-delimited list of SSO types to be enabled, and the order in which they are executed. An empty list indicates that the legacy ordering is to be used. If the list is specified, the legacy options will be ignored. Valid options: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO`, and `siteminder`. If none are desired, specify: `none`
`allowed.cms`	To ensure a secure login and prevent Server-Side Request Forgery, you can create a whitelist of valid CMS names or IPs, along with the port numbers. You are logged into the application only if the value entered during login exactly matches the value in the whitelist. Enter the list of CMS names or IPs along with the port number in the allowed.cms property. For example, `allowed.cms =<cms name or IP>:<port`

Setting	Description
	`number>.` In case you have multiple CMSes to connect to, enter the values separated by comma (,) as shown: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Note** • To log in using either CMS name or IP, add both in the `allowed.cms` property. • As Port number is optional in the login screen, you can choose to omit it in the whitelist. You will then be logged in to the default port. However, if the port number is present in the whitelist and not entered during login, the login fails. Following are the scenarios which do not require the use of whitelist: • If the value of `cms.visible` is set to false and a CMS is set for `cms.default` • If the CMS is clustered and you log in with the cluster name. If you try to log in to a specific cluster (CMS), the CMS name must be present in the `allowed.cms` property. • If login is through Single Sign-On.

17.4.1.3 Fiorified BI Launch Pad properties

The following table lists the settings included in the default `FioriBI.properties` file for the BOE war file. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Note

In BI 4.2 SP5, “Bing.properties” file is renamed to “FioriBI.properties” file. When you update or upgrade to BI 4.2 SP5 from any older version, you need to manually change the name of the Fiorified BI Launch Pad properties file from “Bing.properties” to “FioriBI.properties”, to retain the existing configurations for the Fiorified BI Launch Pad.

Setting	Description
`app.name`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name=BI launch pad`

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>app.name.short</td><td>Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: app.name.short=BI launch pad</td></tr>
<tr><td>app.url.name</td><td>Specifies the URL name of the application, preceded by the "/"" character. Default: app.url.name=/BILaunchpad</td></tr>
<tr><td>authentication.default</td><td>Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting:<table><tr><th>Authentication</th><th>Setting value</th></tr><tr><td>Enterprise</td><td>secEnterprise</td></tr><tr><td>LDAP</td><td>secLDAP</td></tr><tr><td>Windows AD</td><td>secWinAD</td></tr><tr><td>SAP</td><td>secSAPR3</td></tr><tr><td>PeopleSoft</td><td>secpsenterprise</td></tr></table>Default: authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Specifies if users logging into Fiorified BI launch pad have the option to view and change the authentication method. Default: authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>Specifies the visibility of the list of available authentication types in the login screen. Following is the list of available authentication types: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise. From among the list, you can choose to enable or disbale authentication types by either including or excluding the desired authentication types from the Authentication.VisibleList. Default: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise</td></tr>
<tr><td>sap.system.client.visible
authentication.sapSystem
authentication.sapClient</td><td>Specifies the visibility of the SAP System and SAP Client fields, when you select the authentication type as 'SAP'. Default: sap.system.client.visible=true. When sap.system.client.visible is set to sap.system.client.visible=false, you can specify the values for SAP System and SAP Client in the properties file by using authentication.sapSystem= and authentication.sapClient= parameters respectively.</td></tr>
<tr><td>cms.default</td><td>Specifies the default CMS name. Default: cms.default=[name of host machine]</td></tr>
</table>

Setting	Description
`cms.visible`	Specifies if users logging into Fiorified BI launch pad have the option to view and change the CMS name. Default: `cms.visible=true`
`dialogue.prompt.enabled`	Specifies if users should be prompted when navigating away from an input page in a dialog box. Default: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Specifies whether or not to enable token creation for the session after a user logs into BI launch pad. Token will be stored in a cookie. Default: `logontoken.enabled=false`
`SMTPFrom`	Enables or disables the *From* field when scheduling an object to a destination. Default: `SMTPFrom=true` When the value is set to `false` the *From* field will not be displayed and the system attempts to retrieve the *From* email value in the following order: 1. First, from the report default for a report object. 2. Second, from the email address on the user profile of the logged on user. 3. Lastly, from the Job server default.
`url.exit`	Specifies which URL to redirect users after terminating their Fiorified BI launch pad session. This setting applies only to users who have logged into the application through an external verification process.
`disable.locale.preference`	Enables or disables the user from viewing and thus modifying the viewing local preferences for Fiorified BI launch pad. Default: `disable.locale.preference=false`
`extlogon.allow.logoff`	Enables or disables automatically logging off user sessions once they have closed their Fiorified BI launch pad session. Set to false if you want user sessions not to automatically terminate when users log off BI launch pad. Default: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Specifies whether to allow other pages to embed this application (as a frame) without passing a valid embed token. Default: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Specifies a comma-delimited list of SSO types to be enabled, and the order in which they are executed. An empty list indicates that the legacy ordering is to be used. If the list is specified, the legacy options will be ignored. Valid options: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`,

Setting	Description
	`trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO`, and `siteminder`. If none are desired, specify: `none`
`allowed.cms`	To ensure a secure login and prevent Server-Side Request Forgery, you can create a whitelist of valid CMS names or IPs, along with the port numbers. You are logged into the application only if the value entered during login exactly matches the value in the whitelist. Enter the list of CMS names or IPs along with the port number in the allowed.cms property. For example, `allowed.cms =<cms name or IP>:<port number>.` In case you have multiple CMSes to connect to, enter the values separated by comma (,) as shown: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Note** • To log in using either CMS name or IP, add both in the `allowed.cms` property. • As Port number is optional in the login screen, you can choose to omit it in the whitelist. You will then be logged in to the default port. However, if the port number is present in the whitelist and not entered during login, the login fails. Following are the scenarios which do not require the use of whitelist: • If the value of `cms.visible` is set to false and a CMS is set for `cms.default` • If the CMS is clustered and you log in with the cluster name. If you try to log in to a specific cluster (CMS), the CMS name must be present in the `allowed.cms` property. • If login is through Single Sign-On.
upload.file.maxsize.inMB=0	Maximum file size for Local Document upload in MegaBytes and it should be whole number E.g: 10 etc.
upload.file.allowed.formats=	This property is used to control different file types allowed for uploading Local document. refer the SAP Note 2296060 for getting supported file format list.

Setting	Description
	If your defining multiple formats separate each file format followed by comma such as txt,doc,xls.
app.custom.banner.message	Specifies the banner message in the BI Launch pad.
logon.webssoauthnetication.framework=None	This property is used to Enable Web SSO Authentication workflow. The possible values are None, OpenId, and SAML.
openid.restful.url=	This property is used to set the Restful URL which is provided in CMC. For example: `http://<hostname>:<portNo>/biprws`

17.4.1.4 OpenDocument properties

The following table lists the settings included in the default `opendocument.properties` file for the BOE war file. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Description
`app.name`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name=SAP BusinessObjects OpenDocument`
`app.name.short`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name.short=OpenDocument`
`authentication.default`	Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting: **Authentication** / **Setting value** Enterprise / `secEnterprise` LDAP / `secLDAP` Windows AD / `secWinAD` SAP / `secSAPR3` PeopleSoft / `secpsenterprise` Default: `authentication.default=secEnterprise`
`authentication.visible`	Specifies if users logging into OpenDocument have the option to view and change the authentication method. Default: `authentication.visible=false`

Setting	Description
`Authentication.VisibleList`	Specifies the visibility of the list of available authentication types in the login screen. Following is the list of available authentication types: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise`. From among the list, you can choose to enable or disbale authentication types by either including or excluding the desired authentication types from the `Authentication.VisibleList`. Default: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise`

`sap.system.client.visible`
`authentication.sapSystem`
`authentication.sapClient`
	Specifies the visibility of the *SAP System* and *SAP Client* fields, when you select the authentication type as 'SAP'. Default: `sap.system.client.visible=true`. When `sap.system.client.visible` is set to `sap.system.client.visible=false`, you can specify the values for SAP System and SAP Client in the properties file by using `authentication.sapSystem=` and `authentication.sapClient=` parameters respectively.

`cms.default`	Specifies the default CMS name. Default: `cms.default=[name of host machine]`
`cms.visible`	Specifies if users logging into OpenDocument have the option to view and change the CMS name. Default: `cms.visible=true`
`logontoken.enabled`	Specifies whether or not to enable token creation for the session after a user logs into OpenDocument. The token will be stored in a cookie. Default: `logontoken.enabled=false`
`extlogon.allow.logoff`	Enables or disables automatically logging off user sessions once they have closed their OpenDocument session. Set to false if you want user sessions to not automatically terminate when users log off OpenDocument. Default: `extlogon.allow.logoff=true`
`SAPLogonToken.enabled`	Specifies whether or not to allow RESTful Web Service SAP logon tokens to authenticate to the BI platform. The SAP logon token is specified by the X-SAP-LogonToken value in the request header after a successful logon with the RESTful Web Service URL. Default: `SAPLogonToken.enabled=true`
`logon.allowInsecureEmbedding=false`	Specifies whether to allow other pages to embed this application (as a frame) without passing a valid embed token. Default: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Specifies a comma-delimited list of SSO types to be enabled, and the order in which they are executed.

Setting	Description
	An empty list indicates that the legacy ordering is to be used. If the list is specified, the legacy options will be ignored. Valid options: `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO`, and `siteminder`. If none are desired, specify: `none`
`allowed.cms`	To ensure a secure login and prevent Server-Side Request Forgery, you can create a whitelist of valid CMS names or IPs, along with the port numbers. You are logged into the application only if the value entered during login exactly matches the value in the whitelist. Enter the list of CMS names or IPs along with the port number in the allowed.cms property. For example, `allowed.cms =<cms name or IP>:<port number>.` In case you have multiple CMSes to connect to, enter the values separated by comma (,) as shown: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Note** • To log in using either CMS name or IP, add both in the `allowed.cms` property. • As Port number is optional in the login screen, you can choose to omit it in the whitelist. You will then be logged in to the default port. However, if the port number is present in the whitelist and not entered during login, the login fails. Following are the scenarios which do not require the use of whitelist: • If the value of `cms.visible` is set to false and a CMS is set for `cms.default` • If the CMS is clustered and you log in with the cluster name. If you try to log in to a specific cluster (CMS), the CMS name must be present in the `allowed.cms` property. • If login is through Single Sign-On.

17.4.1.5 CMC properties

The following table lists the settings included in the default `cmc.properties` file for BOE.war. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Description
`app.url.name`	Specifies the URL name of the application, preceded by the"/"" character. Default: `app.url.name=/CMC`
`authentication.default`	Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting: **Authentication** / **Setting value** Enterprise / `secEnterprise` LDAP / `secLDAP` Windows AD / `secWinAD` SAP / `secSAPR3` PeopleSoft / `secpsenterprise` Default: `authentication.default=secEnterprise`
`authentication.visible`	Specifies if users logging into the CMC have the option to view and change the authentication method. Default: `authentication.visible=false`
`Authentication.VisibleList`	Specifies the visibility of the list of available authentication types in the login screen. Following is the list of available authentication types: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise`. From among the list, you can choose to enable or disbale authentication types by either including or excluding the desired authentication types from the `Authentication.VisibleList`. Default: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secSAPR3,secpsenterprise`

`sap.system.client.visible`
 	
`authentication.sapSystem`
 	
`authentication.sapClient`
	Specifies the visibility of the *SAP System* and *SAP Client* fields, when you select the authentication type as 'SAP'. Default: `sap.system.client.visible=true`. When `sap.system.client.visible` is set to `sap.system.client.visible=false`, you can specify the values for SAP System and SAP Client in the properties file by using `authentication.sapSystem=` and `authentication.sapClient=` parameters respectively.

Setting	Description
`cms.default`	Specifies the default CMS name. Default: `cms.default=[name of host machine]`
`cms.visible`	Specifies if users logging into the CMC have the option to view and change the CMS name. Default: `cms.visible=true`
`dialogue.prompt.enabled`	Specifies if users should be prompted when navigating away from an input page in a dialog box. Default: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Specifies whether or not to enable token creation for the session after a user logs into the CMC. The token will be stored in a cookie. Default: `logontoken.enabled=false`
`ulr.exit`	Specifies which URL to redirect users after terminating their CMC session. This setting applies only to users who have logged into the application through an external verification process.
`allowed.cms`	To ensure a secure login and prevent Server-Side Request Forgery, you can create a whitelist of valid CMS names or IPs, along with the port numbers. You are logged into the application only if the value entered during login exactly matches the value in the whitelist. Enter the list of CMS names or IPs along with the port number in the allowed.cms property. For example, `allowed.cms =<cms name or IP>:<port number>.` In case you have multiple CMSes to connect to, enter the values separated by comma (,) as shown: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Note** • To log in using either CMS name or IP, add both in the `allowed.cms` property. • As Port number is optional in the login screen, you can choose to omit it in the whitelist. You will then be logged in to the default port. However, if the port number is present in the whitelist and not entered during login, the login fails. Following are the scenarios which do not require the use of whitelist: • If the value of `cms.visible` is set to false and a CMS is set for `cms.default` • If the CMS is clustered and you log in with the cluster name. If you try to log in to a specific cluster (CMS),

Setting	Description
	the CMS name must be present in the `allowed.cms` property. • If login is through Single Sign-On.

17.5 Customizing BI launch pad and OpenDocument logon entry points

You can customize the logon page for BI launch pad and OpenDocument web applications. For example, you can customize the logon page to use a company logo or corporate style sheet, or you can create a customized logon page that enables trusted authentication.

To customize the logon page, modify the `custom.jsp` file stored in the BI launch pad and OpenDocument application areas of the `BOE.war` web application, and then redeploy the `BOE.war` web application to your BI platform system. Users access the custom logon entry point by navigating to a unique URL.

To work with these examples, you need to be familiar with deploying BI platform web applications. For more information, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

17.5.1 BI launch pad and OpenDocument file locations

The BI launch pad and OpenDocument web applications are packaged within the `BOE.war` web archive file. The location of the `BOE.war` archive is defined in the `BOE.properties` file.

The `BOE.properties` file is found here on Windows systems:

- `<BOE_INSTALL_DIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

The `BOE.properties` file is found here on UNIX systems:

- `<BOE_INSTALL_DIR>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

The following tables define the location of common files within the `BOE.war` web archive file for both the BI launch pad and OpenDocument applications.

BI launch pad file locations

> **Note**
>
> The BI launch pad web application was formerly known as InfoView.

File type	Location
Custom logon URL	`http://<servername>:<port>/BOE/BI/custom.jsp`

OpenDocument file locations

File type	Location
Custom logon script	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp`
Directory for additional files	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources`
Custom logon URL	`http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp`

17.5.2 To define a custom logon page

Context

You can customize the entry point to the BI platform logon page. For example, you can create a custom logon page that displays a company logo and uses a corporate style sheet.

Edit the `custom.jsp` file to customize the logon experience for your users, and place supporting files in the `noCacheCustomResources` folder.

This example shows how to create a custom logon page that redirects the user to the standard logon page.

Procedure

1. Create a file that contains your custom logon code, and save it as `custom.js` in the `noCacheCustomResources` folder.

   This example defines a function that redirects the user to the standard logon page, `logon.faces`.

   ```
   function load() {window.location =  "logon.faces";}
   ```

2. Edit the `custom.jsp` file to customize the logon page.

   This example displays a welcome message and a hyperlink that calls the `load` method defined in the `custom.js` file.

   ```
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">
   <%@ page language=  "java" contentType=  "text/html;charset=utf-8"%>
   <html>
     <head> <title>Welcome</title>
     </head>
     <body>
       <script type=  "text/javascript" src=  "noCacheCustomResources/
   custom.js"></script>
       <p>Welcome to ABC corporation.</p>
       <a href= "javascript:load()">Enter</a>
     </body>
   ```

```
</html>
```

3. Redeploy the `BOE.war` web application, and restart the web server.

17.5.3 To add trusted authentication at logon

Context

To enable trusted authentication, set the trusted user as a session attribute in the `custom.jsp` file, and modify authentication settings in a copy of the `global.properties` file. The values of the custom copy of the `global.properties` file override the default values.

> **Note**
>
> Trusted Authentication should not be enabled without HTTPS due to security reasons. If you have enabled Trusted Authentication without https, it is considered as breach of security as the URL is exposed to unauthorized users. To avoid security breach, the user's information can be validated with a valid certificate. For more information, refer to 1388240.

Procedure

1. Edit the `custom.jsp` file to set a session attribute that defines the trusted user.

```
request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
```

2. Create a custom copy of the `global.properties` file by copying `WEB-INF\config\default\global.properties` to `WEB-INF\config\custom\global.properties`.
3. Modify `WEB-INF\config\custom\global.properties` to enable Single Sign-on (SSO).

```
sso.enabled=true
```

4. Modify `WEB-INF\config\custom\global.properties` to set trusted authentication parameters, including the trusted user session variable, and the shared secret.

   Replace `"..."` with the shared secret for your system.

```
trusted.auth.user.param=TrustedUserAttribute
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.shared.secret="..."
```

   For more details, see the related topic on configuring trusted authentication for web applications.
5. Redeploy your web application, and restart the web server.
6. In the CMC, enable trusted authentication.

   On the *Authentication* tab, double-click *Enterprise*, and then select the check box *Trusted Authentication is enabled*.

Related Information

Enabling Trusted Authentication [page 243]
To configure Trusted Authentication for the web application [page 253]

17.6 Customizing application user interfaces

Some application user interfaces can be customized through the CMC.

In the Central Management Console, you can customize the appearance of some applications. For example, you can toggle user interface elements.

17.6.1 Web Intelligence

17.6.1.1 Customizing Web Intelligence interface elements by user groups and folders

Customization allows you to hide multiple interface elements to simplify the way end-users interact with the application, depending on user groups and folders containing Web Intelligence documents. You can hide data sources types, edit mode toggle, turn-off the auto refresh feature, and many more.

By default, every interface element is enabled. If you want to hide them, you can do so in the Central Management Console. The table below lists the user interface elements you can hide.

Features List	Description
Mode	Hides the available modes the user can access through the drop-down button. • Reading To hide the Reading mode from the drop-down button. • Design To hide both the Design and Structure modes from the drop-down button. • Data To hide the Data mode from the drop-down button. If all modes are disabled, then documents can only be opened in Reading mode.
Location	Hides a whole category of data sources. Categories you can disable are: • BI Platform Repository • Local (only available in Rich Client) • Web Services • Google Drive • Microsoft OneDrive

Features List	Description
Data Source	In Design mode, you can restrict the data sources available in the *Select a Data Source* and the *Change Source* dialog boxes. The data sources you can disable are: • Universes • Web Intelligence documents • Excel files • Text files • SAP BW • SAP HANA views • Free Hand SQL queries • OData • Google Spreadsheet
Query	• Refresh In Reading mode, hides the *Data* section in the toolbar. In Design mode, hides the *Refresh* dropdown menu, the *Refresh All* command, the *Run* button and its dropdown menu in the Query Panel. • Advanced Refresh In Design mode, hides the *Advanced Refresh* command in the *Refresh* dropdown menu. • Auto-Refresh Hides the *Auto-Refresh* option in the Presentation Mode. • Change Source In Design mode, hides the ability to change the document's data sources.
Data	In Data mode, hides the Combine Cubes features.
Analysis	• Drill In both Reading and Design mode, hides the *Drill* checkbox in the Analyze section of the toolbar, drill filters in the *Filter Bar*. Also, in the report, values that can be drilled are not displayed as hyperlinks and the drill actions and icons available for these values are hidden. In Design mode, hides the drill filters in the *Build* panel, under *Data Filters*. • Track Data Changes In both Reading and Design mode, hide the *Track Data Changes* and *Show Changes* from the toolbar.
Documents	• *New*, *Open*, *Save*, *Favorites*, *Presentation Mode*. Hides the corresponding buttons from the toolbar. • Comments In both Reading and Design modes, hide the *Comments* tab in the side panel, and the *Comments* command in the contextual menu. • Shared Elements In Design mode, hide the *Shared Elements* tab in the side panel, and the *Shared Elements* command in the *Insert* section of the toolbar.

Features List	Description
Export To	In any modes, hides the possibility to export documents report and cubes to: • Excel • PDF • HTML • TXT • CSV • WIDX
Generate Link	In Design mode, hides the ability to create OpenDocument link and generate OData links for queries and individual report elements from contextual menus.
Schedule & Publishing	Hides the possibility to schedule and publish documents to TXT, XLS, PDF, HTML, MHTML, CSV, and WIDX.

17.6.1.1.1 Customization interface

You can select individual folders so that the documents they contain automatically benefit from the customization. Simply select one or more folders in the *Customized folders* area, and move on to the *Features* tab to start customizing. By default, the customization applies to every document in the folder you have selected.

The *Features* tab lists all the features you can enable or disable. Use the dedicated checkboxes to toggle them on or off.

17.6.1.1.2 Customization rules

The following rules are used to define customizations to apply to a user:

- If the user belongs to different groups, you can define how the customization applies. By default, only the customization defined to the group whose ID is lower applies. The customization defined for the other groups containing the user does not apply.
  You can change and define to hide a feature if it is denied for at least one group containing the user.
- For nested folder structure, the immediate parent folder of the document that has been added in the list of customized folders defines customizations for the document for user interface elements, features, and extensions.
- The customization defined for Default Folders applies for the documents stored in Personal Documents and Inboxes, and for documents for which the parent folder is not customized.
- The customization defined for user interface elements have priority over customization defined for features as feature is only a shortcut to enable all user interface elements.
- Scenario: When the customization elements are displayed as a tree list and you disable a node on a system. Here, if you upgrade this system with a newer version of the product having new items in the nodes, then by default these items are activated even if the upper node is disabled.

17.6.1.1.3 To modify the customization aggregation behavior

Procedure

1. Log into the CMC
2. Go to the *Applications* page.
3. Double-click *Web Intelligence* or select *Web Intelligence* and click *Properties* in the toolbar.
4. In the *Web Intelligence Customization* section, select:
    1. *Hide features disabled for the lowest ID group containing the user*: To select the default algorithm used in the previous releases.
    2. *Hide features disabled for at least one group containing the user*: To hide a feature if it is denied for at least one group containing the user.

17.6.1.1.4 To customize the Web Intelligence interface appearance

Context

You can customize the appearance of the Web Intelligence user interface by hiding menu items, subitems, and features for a selected user group and document folder.

Procedure

1. Log into the CMC as an Administrator.
2. From the *Organize* list, select *Users and Groups*.
3. In the *Group Hierarchy* list, select a user group.
4. In the *Actions* list, select *Customization*.
5. In the *Customized folders* section, do one of the following:

Option	Description
To define a default customization	1. Select *Default Folders* in the *Customized folders* area.
To add the document folders for which you want to apply customization for the selected user group	1. Click *Add Folder*. 2. Select the folders. The folders displays in the *Customized folders* area.

Option	Description
To avoid redefining the same customization for other folders	1. In the *Customized folders* area, select the folder from which you want to copy the customization. 2. In the dropdown list, click *Duplicate Customization*. 3. Select the folder to which you want define the customization. 4. Click *Paste Customization*. 5. Go to step 7.
To remove the customization for a specific folder	1. In the *Customized folders* area, select the folder. 2. In the dropdown list, click *Remove Folder*. 3. Go to step 7. **Note** You can't remove *Default Folders*.

6. Select or deselect items in the *Features* tab to display or hide them in Web Intelligence.

   If you deselect all children of a parent item, the parent item is also deselected and hidden in Web Intelligence. For more information, check out Customizing Web Intelligence interface elements by user groups and folders [page 695].
7. Click *Save & Close*.

Results

When you save the customization, all users of the selected group will see these changes the next time they log on to BI launch pad and open Web Intelligence.

> **Note**
>
> We recommend that you log on to BI launch pad as a user from the group you have just customized, start Web Intelligence, and verify that the interface corresponds to your customization settings.

17.6.1.2 Web Intelligence content alignment

Choose the way document content will be aligned (left-to-right or right-to-left) when users create Web Intelligence documents.

For the Rich Client interface, the content alignment is determined by the locales set in the BI launch pad preferences:

- The system uses right-to-left alignment only when both the Preferred Viewing Locale and Product Locale are set to right-to-left languages.
- In all other cases, the content alignment is left-to-right.

> **Note**
>
> For information about how to set locales, see the *Business Intelligence Launch Pad User Guide*.

> **Note**
>
> Content alignment applies only at document creation time, and doesn't affect existing documents.

17.6.1.3 Enabling Web Intelligence User Interface Extension Points for specific user groups

You can configure Web Intelligence rights to allow selected user groups to access customized interface extensions. Refer to the *SAP BusinessObjects BI Developer's Guide for Web Intelligence and the BI Semantic Layer* for more information about extension bundles and the REST web services API calls that are available.

17.6.1.3.1 To enable Web Intelligence User Interface Extension Points

Prerequisites

- You have created and deployed the appropriate extension in your installation. Deploy one extension for each extension feature (for example, Custom Button, or Save as HTML).
- You have have added the extension to the list of trusted URLs. If you havent, check the To add trusted URLs to the Authorized URLs list [page 652] section.

Procedure

1. Log in to the CMC as an Administrator.
2. From the *Organize* list, select *Users and Groups*.
3. In the *Group Hierarchy* list, select a user group.
4. In the *Actions* list, select *Customization*
5. Click the *Extensions* tab and do one of the following:

Option	Description
To add an OSGi extension deployed on the BI platform and its application server	Select the custom extensions that you want the users to use.
To add a non-OSGi extension deployed either on the BI platform application server or on an external application server	1. Click *Add*. 2. Enter the Extension URL. This is the URL of the JSON file.

Option	Description

	Note
	Replace any blank space of the URL with **%20**.
	Examples:
	• Apache Tomcat application server:
	`http://myserver/webiextension/extension/SAP/RayLight_Embedded/extension.json`
	• External application server:
	`http://www.mysite.org/documents/web/extension/Custom%20Button/extension.json`
	3. Select *Set proxy information if required* by your application server and enter server name and port number.
	4. Select either *No authentication* or *Basic authentication* if required by your application server and enter user name and password.
	5. Click *OK* and select the extension.
	6. Click *Save*.

To modify an extension details	Click *Modify*.
To remove an extension from the CMC	Click *Remove*.

6. Click *Save & Close*.

Results

The enabled extensions are available to the selected user group when opening a document located in the selected folder. The extension points are available to all Web Intelligence application clients: web, Java Applet, and Rich Client.

17.6.2 BI launch pad

17.6.2.1 To enable cleaning prompts values in the Schedule dialog box

When scheduling a Web Intelligence document based on a BEx query that contains SAP BW prompts, BI launch pad users can clear a prompt value so that it will be obtained by the SAP BW data source variable when the document runs, or fix it before running the scheduling job.

Context

The procedure below allows you to display two radio buttons in the user interface:

- *Use Dynamic Value*: Let the SAP BW data source process the value.
- *Use Constant Value*: Enter a fixed a value.

Procedure

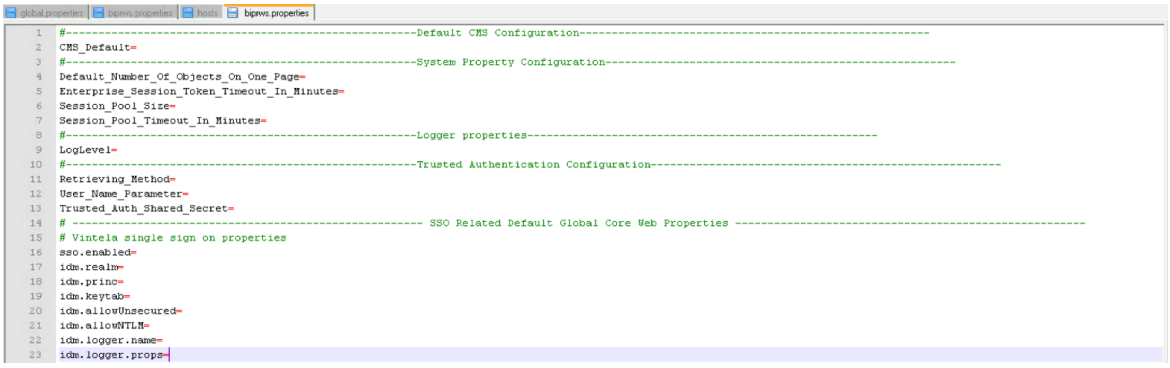
1. Perform one of the following actions in the `<InstallDir>\<WebAppServer>\webapps\BOE\WEB-INF\config\custom` folder:
   - If an `AnalyticalReporting.properties` file is located in the folder, open the file in a text editor.
   - If no `AnalyticalReporting.properties` file exists in the folder, create a file with that file name, and open it in a text editor.
2. Perform one of the following actions in the `AnalyticalReporting.properties` file:
   - If the file already existed, locate the `bex.dynamic_variable.schedule` property in the file, and ensure that its value is set to `true`.
   - If you created the `AnalyticalReporting.properties` file, add `bex.dynamic_variable.schedule=true` to the end of the file..
3. Save and close the file, and then restart the web application server.

17.7 Configuring BI Platform RESTful Web Services on Web Server

To customize the configuration for RESTful web services, follow the steps below:

1. Copy the file: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\default\biprws.properties` to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` and then open it for editing.

Modify the parameters as required.



Given below is a table describing the properties shown in the screenshot.

Property	Description	Default Value

`CMS_Default`	The user can provide name of the CMS and its port number, or the cluster name as well.
	Example:
	`CMS_HOST_NAME:CMS_PORT_NUMBER`
	Or
	`@CMS_CLUSTER_NAME`
		0

`Default_Number_Of _Objects_On _One_Page`	The number of entries that will be listed per page. You can override this setting with the `&pageSize=<m>` parameter in the RESTful Web Services SDK.	50
`Enterprise_Session_ Token_Timeout_In_Minutes)`	The expiry time a logon token will remain valid for. Beyond this time, you need to generate a new logon token.	60
`Session_Pool_Size`	The number of cached sessions that can be stored at any point in time. The session pool caches active RESTful web service sessions so they can be reused when a user sends another request that uses the same logon token in the HTTP request header.	1000
`Session_Pool_Timeout_In_Minutes`	The time in minutes after which the cached sessions will expire.	2

Property	Description	Default Value
`LogLevel`	Enables logging and sets the level of severity and detail to *None* (only critical events logged), *Low* (startup, shutdown, start and end request messages), *Medium* (error, warning and most status messages) or *High* (Nothing excluded. It is used for debugging only. The CPU usage may increase, thereby impacting performance). The available menu choices are: • `Unspecified` • `None` • `Low` • `Medium` • `High`	Unspecified
Log_Location	The location of the log file that records usage logs for the machine, where the BI platform is hosted. **Note** • A new folder is created if you provide the file path to a folder that does not exists. • The log file's location is set to default location if the location is not specified in the biprws.properties file.	Unspecified

Property	Description	Default Value
`Retrieving_Method`	The menu that specifies which query method will be used to retrieve trusted authentication logon tokens when using the RESTful web service API/logon/trusted. • `HTTP_HEADER` is used for GET queries with the request header accept=application/xml (or application/json). • `QUERY_STRING` is used to add a logon name to the end of a URL query using the RESTful Web Service API, for example /logon/trusted/?user=johndoe. • `COOKIE` is used when the login name is retreived from a web browser cookie. The domain, name, value and path must be stored in the cookie	`HTTP_HEADER`
`User_Name_Parameter`	The label used to identify the trusted user for the purposes of retrieving a logon token.	`X-SAP-TRUSTEDUSER`
`Trusted_Auth_Shared_Secret`	The string value generated by following the steps mentioned in the sectionRegenerating a shared secret value [page 382].	Unspecified
`Basic_Auth_Supported`	Enables basic authentication on Tomcat web server. Possible values are `True` or `False`.	Unspecified
`Basic_Auth_Type`	Sets the authentication to `secEnterprise`, `secLDAP`, `secSAPR3`, or `secWinAD` to support basic authentication.	`secEnterprise`

2. Restart Tomcat.

18 Managing Connections and Universes

18.1 Managing connections

A connection is a named set of parameters that defines how one or more SAP BusinessObjects applications can access relational or OLAP databases. Connection details such as server name, database, user name, and password, can be stored securely in the BI platform repository in the Connections folder.

Designers define universes based on connections. Users of query, analysis, and reporting applications access the database via the universe without needing to know about the underlying data structures in the database.

You can create connections using the following applications:

- **Information Design Tool**: Connections can be created locally and then published to the repository, or created and edited directly in the repository.
- **Central Management Console (CMC)**: Only OLAP connections can be created in CMC.

> ⓘ Note
>
> Connections are shared with other applications, such as SAP Crystal Reports, SAP BusinessObjects Web Intelligence, Web Intelligence Rich Client, and Information Design Tool.

> ⓘ Note
>
> SAP BusinessObjects *Analysis edition for OLAP* (AOLAP) is removed as part of SAP BI 2025.
>
> You can also create new OLAP connections from *Central Management Console* > *Connections*

You grant rights to allow users to create, edit, and delete connections.

You grant user access to universe connections and allow users to create and view documents that use universes and connections.

Related Information

Managing security settings for objects in the CMC [page 123]
Connection rights [page 1053]

18.1.1 To delete a universe connection

Context

> → Tip
>
> It is also possible to delete connections in the information design tool.

Procedure

1. In the *Connections* area, select a universe connection from the list.
2. Click *Manage* > *Delete* .

18.1.2 OLAP data source connections

OLAP connections are based on the *SAP BICS* client. You can use them to connect to OLAP data sources such as SAP BW (including BW4HANA and SAP S/4HANA), SAP HANA, SAP Datasphere, Microsoft Analysis Services, or Oracle Essbase.

OLAP Provider Support

Our OLAP provider support includes the following:

SAP

- SAP BW (including BW/4HANA and S/4HANA)
- SAP HANA (On-Premise and Cloud)
- SAP Datasphere

Microsoft

- Microsoft Analysis Services (2016, 2017, 2019)

Oracle

- Hyperion Essbase 11.x

Additionally, you can edit OLAP connections created in the *Information Design Tool (IDT)*.

18.1.2.1 Creating OLAP data source connections

18.1.2.1.1 To create a new connection object for a data source system

Procedure

1. Log on to the Central Management Console.
2. In the Organize area in the CMC, select *Connections*.
3. Select the folder where you want your new connection to be placed.

   You can select the Connections folder or any subfolder, or create a new subfolder.
4. Click *New OLAP Connection*.
5. In *Choose Connection Type*, select the OLAP Vendor and Provider from the list.
6. Click *Next* to go to Configure Connection Properties.
7. Enter a *Name* and optionally type a *Description* for your connection.
8. Enter the provider-specific server information, such as the server's name and other required information in *Server Settings*.
9. Select an authentication mode in *Authentication Settings*.
10. Click *Create Connection* to create the connection.

    The connection is now available for users to consume in other applications, such as SAP Crystal Reports, SAP BusinessObjects Web Intelligence, Web Intelligence Rich Client and Information Design Tool.

18.1.2.1.2 To create a new connection object for a cube or a query

Procedure

1. Log on to the Central Management Console.
2. In the Organize area in the CMC, select *Connections*.
3. Select the folder where you want your new connection to be placed.

   You can select the Connections folder or any subfolder, or create a new subfolder.
4. Click *New OLAP Connection*.
5. In *Choose Connection Type*, select the OLAP Vendor and Provider from the list.

6. Click *Next* to go to Configure Connection Properties.
7. Enter a *Name* and optionally type a *Description* for your connection.
8. Enter the provider-specific server information, such as the server's name and other required information in *Server Settings*.
9. Select an authentication mode in *Authentication Settings*.
10. In the Cube Browser, select the cube, query, or view that you want to use for this connection, and then click *Select*.

    > ⓘ Note
    >
    > The Cube Browser will function properly only when all necessary connection details are configured accurately in the Server Settings and Authentication Settings. If browsing cubes fails, it is recommended to test the connection first to ensure a successful connection to the database.

11. You can manually browse through the folders in the Cube Browser to locate your cube, query, or view, or you can search for it.
12. Click *Create Connection* to create the connection.

    The connection is now available for users to consume in other applications, such as SAP Crystal Reports, SAP BusinessObjects Web Intelligence, Web Intelligence Rich Client, and Information Design Tool.

18.1.2.1.3 Finding a cube or a query

The Cube Browser provides search capabilities to help you locate a cube, SAP BW query, or SAP HANA view within a data source system.

Searching in the Cube Browser

You can type a search term in the text field for Name, Description, or Technical Name at the top of the Cube Browser to find a cube, SAP BW query, or SAP HANA view.

> ⓘ Note
>
> Search terms are not case-sensitive. Searching for **sales** is the same as searching for **Sales** or **SALES** or **saLEs**.

18.1.2.1.4 To copy a connection object

Procedure

1. Log on to the Central Management Console.

2. In the Organize area in the CMC, select *Connections*.
3. Select the connection that you want to copy.
4. Click *Copy OLAP Connection* or right-click on an existing connection and select *Organize* > *Copy*.
5. Enter a *Name* and optionally type a *Description* for your connection.
   You can choose to save the copied connection now or make changes to the connection settings.

   > **Note**
   >
   > You may need to re-enter the password if you are using the *Use specified user name and password* authentication mode.

6. Click *Save* to create the connection.
   The connection is now available for users.

18.1.2.1.5 Authentication

You can set the type of authentication to use when users create new OLAP connection.

You can choose from the following authentication types when you create an OLAP connection in the CMC.

These methods are used to authenticate the user's login credentials when accessing the data source:

- **Use Specified User Name and Password**:
  Uses the *User Name* and *Password* parameters defined for the connection. The administrator enters a specific user name and password, which will be stored as part of the connection object.
- **Use BusinessObjects Credential Mapping**:
  Uses the database credentials associated with the user's account defined on the Central Management Server (CMS) to connect to the data source. The database credentials are set in the User's Properties in the Central Management Console. For more information, see the *SAP BusinessObjects Business Intelligence Platform Administrator's Guide*.
- **Use Single Sign On**:
  This authentication mode is used to support end-to-end single sign-on defined in the Central Management Server (CMS). If you use an external authentication source (for example LDAP), the CMS and the data source must be configured to use this external authentication source.

For more information on single sign on, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

These OLAP providers support single sign-on:

- SAP BW
- SAP HANA
- SAP Datasphere
- Microsoft Analysis Services

For SAP HANA, single sign-on is implemented using Security Assertion Markup Language (SAML). SAML must be configured in both the BI platform and SAP HANA. User mapping between BI platform users and SAP HANA users must also be configured in SAP HANA.

For information about configuring single sign on with SAP HANA, refer to the “Configuring SAP HANA single sign-on” section of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*. For information about configuring SAP HANA SAML settings, refer to the *SAP HANA Security Guide*. These guides are available on the SAP Help Portal at http://help.sap.com.

> **Note**
>
> SAP Datasphere supports only SSO (Single Sign On) as the authentication method; no other authentication types are supported.

18.1.2.2 To edit a connection object

Procedure

1. Log on to the Central Management Console.
2. In the Organize area in the CMC, select *Connections* .
   A list of existing connections is displayed.
3. Select the connection that you want to edit and click *Edit Connection* or right-click on an existing connection and select *Organize* > *Edit* .

   > **Note**
   >
   > - You may need to re-enter the password if you are using the *Use specified user name and password* authentication mode.
   > - If you do not have "Add objects to the folder" permission in the BI platform system, you cannot edit a connection, and the *Edit Connection* button is unavailable.
   > - If you do not have “Download connection locally” permission in the BI platform system, you cannot edit a connection.

   You can now change the contents of any of the fields to reconfigure your OLAP connection
4. Click *Save* to save the connection settings.
   The connection is now available for users.

18.1.2.3 To delete a connection

Context

If a data source connection is no longer being used, you can delete the connection.

Procedure

1. Log on to the Central Management Console.
2. In the Organize area in the CMC, select *Connections*.
   A list of existing connections is displayed.
3. Select the connection that you want to delete.
4. From the menu, select *Manage* > *Delete* or right-click on an existing connection and select *Delete*.

18.1.2.4 To move a connection to another folder

Procedure

1. Log on to the Central Management Console.
2. In the Organize area in the CMC, select *Connections*.
3. Select the connection that you want to move.
4. Click *Organize* > *Move To* or right-click on an existing connection and select *Organize* > *Move To*.
5. Select a destination folder, and click *Move*.

18.1.2.5 Data source connection setting parameters

This section describes the provider-specific connection settings for all supported OLAP data sources.

18.1.2.5.1 Connection settings for SAP Business Warehouse data sources

Login parameters for SAP BW and ERP connections

Connecting to an application server

To connect directly to a SAP BW application server, choose the application server for Logon Mode. The following information is required to establish a connection to an application server:

- Client: The three-digit client number
- Application Server: Name or IP address of the application server
- System Number
- System ID: The three-character SAP system ID

Connecting to a message server

You can leverage SAP load balancing by connecting to a message server. To connect to a message server, choose the Message Server for Logon Mode. The following information is required to establish a connection to a message server:

- Client: The three-digit client number
- Message Server: The name or IP address of the SAP message server used for load balancing.
- System ID: The three-character SAP system ID
- Logon Group: Name of the Logon group; a set of dedicated application servers used to log on.

Save Language

Specifies the language to use for the connection:

- If you select the *Save Language* option, the value from the *Language* parameter is used.
- If you choose not to save the language, the value from the user's session (Preferred Viewing Locale) is used.

Authentication mode

The method used to authenticate the user's login credentials when accessing the data source:

- **Use Specified User Name and Password**:
  Uses the User Name and Password parameters defined for the connection.
- **Use BusinessObjects Credential Mapping**:
  Uses the database credentials associated with the user's account defined on the Central Management Server (CMS) to connect to the data source. The database credentials are set in the User's Properties in the Central Management Console. For more information, see the *SAP BusinessObjects Business Intelligence platform Administrator's Guide*.
- **Use Single Sign On** :
  This authentication mode is used to support end-to-end single sign on defined in the Central Management Server (CMS). If you use an external authentication source (for example LDAP), the CMS and the data source must be configured to use this external authentication source.

For more information on single sign on, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

Maximum Parallel Queries

Executes maximum number of queries accessing data for a particular connection, concurrently with other connections.

When you refresh a document with multiple data providers, the *Maximum Parallel Queries* setting executes queries accessing data simultaneously and concurrently with other connections.

For more information on refreshing queries in parallel, see the *SAP BusinessObjects Web Intelligence User's Guide*.

18.1.2.5.2 Connection settings for SAP Datasphere data sources

Login parameters for SAP Datasphere connections

Data source

Datasphere tenant URL `http(s)://<Server:port>`

Authentication mode

The following method is used to authenticate the user's login credentials when accessing the data source:

- **Use Single Sign On**: This authentication mode is used to support end-to-end single sign-on enforced by OAuth authentication and defined in the Central Management Server (CMS).
  The authorizations for this authentication mode must be declared in the Central Management Console (CMC), by defining an Authorization Server Configuration.
  With this authentication mode, you need to select the Authorization Reference you have defined in the CMC and generate the OAuth tokens to connect metadata and data at runtime.
  For more information on single sign-on, see the *SAP BusinessObjects Business Intelligence Platform Administrator's Guide*.

Authorization reference

The Authorization Server Configuration defined in the Central Management Console (CMC) to authenticate to the authorization server via OAuth if the Authentication Mode is Use single sign-on with OAuth 2.0.

For more detail to configure an authorization server and test authorization server configuration, refer to the Authorization Server Configuration section in *Business Intelligence Platform CMC Help Guide*.

Save Language

Specifies the language to use for the connection:

- If you select the *Save Language* option, the value from the *Language* parameter is used.
- If you choose not to save the language, the value from the user's session (Preferred Viewing Locale) is used.

Maximum Parallel Queries

Executes maximum number of queries accessing data for a particular connection, concurrently with other connections.

When you refresh a document with multiple data providers, the *Maximum Parallel Queries* setting executes queries accessing data simultaneously and concurrently with other connections.

For more information on refreshing queries in parallel, see the *SAP BusinessObjects Web Intelligence User's Guide*.

18.1.2.5.3 Connection settings for Microsoft Analysis Services data sources

Login parameters for Microsoft Analysis Services data sources

These connection settings are configurable with Microsoft OLAP data sources such as Microsoft SQL Server 2016 Analysis Services.

Server: Connect to a cube on an Analysis Services server by providing the URL to the IIS instance that processes XMLA requests for the server. For example: `http://<IIS servername>/olap/msmdpump.dll`, where `<IIS servername>` is the name of your IIS server. You can use localhost as the IIS server name if everything is installed on one server.

Authentication mode

The methods used to authenticate the user's login credentials when accessing the data source:

- **Use Specified User Name and Password**:
  Uses the User Name and Password parameters defined for the connection.
- **Use BusinessObjects Credential Mapping**:
  Uses the database credentials associated with the user's account defined on the Central Management Server (CMS) to connect to the data source. The database credentials are set in the User's Properties in the Central Management Console. For more information, see the *SAP BusinessObjects Business Intelligence Platform Administrator's Guide*.
- **Use Single Sign On**:
  This authentication mode is used to support end-to-end single sign on defined in the Central Management Server (CMS). If you use an external authentication source (for example LDAP), the CMS and the data source must be configured to use this external authentication source.

For more information on single sign on, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

Save Language

Specifies the language to use for the connection:

- If you select the *Save Language* option, the value from the *Language* parameter is used.

- If you choose not to save the language, the value from the user's session (Preferred Viewing Locale) is used.

Maximum Parallel Queries

Executes maximum number of queries accessing data for a particular connection, concurrently with other connections.

When you refresh a document with multiple data providers, the *Maximum Parallel Queries* setting executes queries accessing data simultaneously and concurrently with other connections.

For more information on refreshing queries in parallel, see the *SAP BusinessObjects Web Intelligence User's Guide*.

> **Note**
>
> When attempting to open an existing connection to a Microsoft Analysis Services (MSAS) version that is no longer supported in BI 2025, the following error message is displayed:
>
> "This release does not support MDX-based OLAP connections for SAP Business Planning and Consolidation for Microsoft platform, SAP BusinessObjects Financial Consolidation, and SAP BusinessObjects Profitability and Costs Management. Please, for more details, refer to *SAP Knowledge Base Article 3509206* on the SAP Support Portal. "

For more information, see Microsoft's documentation for Analysis Services, which is available either as part of your Microsoft SQL Server Analysis Services installation, or on the MSDN Website at http://msdn.microsoft.com/library/ .

For information about configuring HTTP access to SQL Server Analysis Services, see this Microsoft article: http://technet.microsoft.com/en-us/library/gg492140.aspx

18.1.2.5.4 Connection settings for SAP HANA data sources

Login parameters for SAP HANA data sources

You can create SAP HANA OLAP connections based on BICS InA to access an SAP HANA Cloud system or also an SAP HANA on-premises system. In SAP HANA OLAP connections, the following connection types are possible:

- **On Premise**: connection type (default) to configure the connection on an SAP HANA on-premises system.
- **On Cloud**: connection type to connect to data on an SAP HANA Cloud system.

These are common connection settings for SAP HANA data sources, based on connection type selection connection setting parameters will change.

Authentication mode

The following methods are used to authenticate the user's login credentials when accessing the data source:

- **Use Specified User Name and Password**:

Uses the User Name and Password parameters defined for the connection.

- **Use BusinessObjects Credential Mapping**:
  Uses the database credentials associated with the user's account defined on the Central Management Server (CMS) to connect to the data source. The database credentials are set in the User's Properties in the Central Management Console. For more information, see the *SAP BusinessObjects Business Intelligence Platform Administrator's Guide*.
- **Use Single Sign On**:
  This authentication mode is used to support end-to-end single sign on defined in the Central Management Server (CMS). If you use an external authentication source (for example LDAP), the CMS and the data source must be configured to use this external authentication source.

For more information on single sign on, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

Save Language

Specifies the language to use for the connection:

- If you select the *Save Language* option, the value from the *Language* parameter is used.
- If you choose not to save the language, the value from the user's session (Preferred Viewing Locale) is used.

Maximum Parallel Queries

Executes maximum number of queries accessing data for a particular connection, concurrently with other connections.

When you refresh a document with multiple data providers, the *Maximum Parallel Queries* setting executes queries accessing data simultaneously and concurrently with other connections.

For more information on refreshing queries in parallel, see the *SAP BusinessObjects Web Intelligence User's Guide*.

18.1.2.5.4.1 SAP HANA On-premise

Protocol

In SAP HANA OLAP connections, the following protocols are possible to access the SAP HANA on-premises system:

- HTTP protocol
- JDBC protocol

Connection parameter setting based on protocol

- **HTTP protocol (default)**: This option is only available for SAP HANA on-premises system.
  - Set the *Data Source* URL in the format: `http(s)://<host>:<port>`
  - You can use the Smart Refresh feature of Web Intelligence in selecting the *Allow SQL access to the remote database* option.
  - **Allow SQL access to the remote database**:
    When *Allow SQL Access to the remote database* is enabled, two options are available:
    - Use multi-tenant
    - Use specified host and part (failover)

    For more details, see Configuring SQL access on SAP HANA HTTP [page 719].
  - **Properties for the Use multi-tenant option**:
    - **Database Host Name**: Specify the SAP HANA server name.
    - **Database Instance Number**: Provide the instance number for the connection.
    - **Database Name**: Specify the database name of the remote SAP HANA server instance.
  - **Properties for the Connect to port or failover option**:
    Server: Define the remote SAP HANA database server(s) in the format `<server>:<port>` or `<server>:<port> [<server2>:<port2>]`
- **JDBC protocol**: In JDBC protocol, the Smart Refresh feature is not available. This means the *Allow SQL access to the remote database* option is not available; this option is available for both SAP HANA on-premises and SAP HANA cloud. The following action is possible:
  - Set the *Data Source* URL under the format: `<host>:<port>`.
    Note that `jdbc:sap://<host>:<port>` is also accepted.

  The *Use SSL* field is only available in this protocol for SAP HANA on-premises connection type.

18.1.2.5.4.2 SAP HANA On-Cloud

Data Source

- Set the *Data Source* URL under the format: `<host>:<port>`.
  Note that `jdbc:sap://<host>:<port>` is also accepted.

> **Note**
>
> - The Smart Refresh feature is not available. This means the *Allow SQL access to the remote database* option is not available for SAP HANA cloud.
> - For SAP HANA Cloud connection types, the *Use SSL* is forced to *True* in the backend.

18.1.2.5.4.3 Configuring SQL access on SAP HANA HTTP

You can configure SQL access on SAP HANA HTTP connections to directly connect a remote SAP HANA database instance when you refresh a document. This increases the performance at runtime on this type of connection.

When executing queries on SAP HANA, Web Intelligence and the semantic layer use the best SAP HANA access (between HTTP and SQL access) according to the query specifications.

To do this, you must configure SQL access on SAP HANA HTTP connections to directly connect a remote SAP HANA database instance at refresh time. The SQL access option does not impact the SAP HANA variable support level on SAP HANA HTTP connections, and the query panel capabilities are unchanged.

> **Note**
>
> This connection configuration does not work for UNX universes on SAP HANA HTTP connections. It only works for the direct access to SAP HANA from SAP BusinessObjects Web Intelligence.

To use this feature:

- You must have access to SAP HANA HTTP.
- SQL access to your remote SAP HANA database is granted for users who use the SAP HANA HTTP connections in Web Intelligence and the semantic layer.
- If your SAP HANA XS server is configured for HTTPS/SSL with a signed certificate, then the SQL access to the remote SAP HANA database should be also configured for SSL connections (see SAP HANA documentation on how to configure SSL on a SAP HANA server).
- If your SAP HANA HTTP connection is using SAML SSO connection, then the SQL access to the remote SAP HANA database should be also configured for SSO connections.

For more information, see the documentation for SAP HANA available on the SAP Help Portal at SAP HANA Platform | SAP Help Portal.

18.1.2.5.5 Connection settings for Oracle Essbase data sources

The following connection settings are configurable with Oracle Hyperion Essbase 11.X:

Server

Specify the URL for the Oracle Essbase server, including the port if required. If no port is specified, the default port (1423) is used.

Authentication mode

The following methods are used to authenticate the user's login credentials when accessing the data source:

- **Use Specified User Name and Password**:
  Uses the User Name and Password parameters defined for the connection.
- **Use BusinessObjects Credential Mapping**:

Uses the database credentials associated with the user account defined on the Central Management Server (CMS) to connect to the data source. The database credentials are set in the User's Properties in the Central Management Console.

For more information, see the *SAP BusinessObjects Business Intelligence Platform Administrator's Guide*.

Save Language

Specifies the language to use for the connection:

- If you select the *Save Language* option, the value from the *Language* parameter is used.
- If you choose not to save the language, the value from the user's session (Preferred Viewing Locale) is used.

18.2 Managing universes

A universe is an organized collection of metadata objects that enables business users to analyze and report on corporate data in non-technical language. These objects include dimensions, measures, hierarchies, attributes, pre-defined calculations, functions, and queries. The metadata object layer is built on a relational database schema or an OLAP cube, so the objects map directly to the database structures. A universe includes connections to the data sources so that users of query and analysis tools can connect to a universe and run queries and create reports using the objects in a universe without needing to know about the underlying data structures in the database.

You can create universes with the following tool:

- The information design tool. Universes created with this tool are based on the new semantic layer. They are distinguished by the .unx extension and are therefore called .unx universes. The .unx universes are authored locally and published to the repository Universes folder. Designers can define object-level security using the information design tool security editor.

You grant users application rights and universe rights to allow them to create, edit, and delete universes, as well as design security on universes.

You grant users universe rights to allow them to create and view documents that use universes.

Related Information

Managing security settings for objects in the CMC [page 123]
Information design tool [page 1057]
Universe (.unx) rights [page 1050]

18.2.1 To delete universes

Context

> → Tip
>
> It is also possible to delete universes in the information design tool.

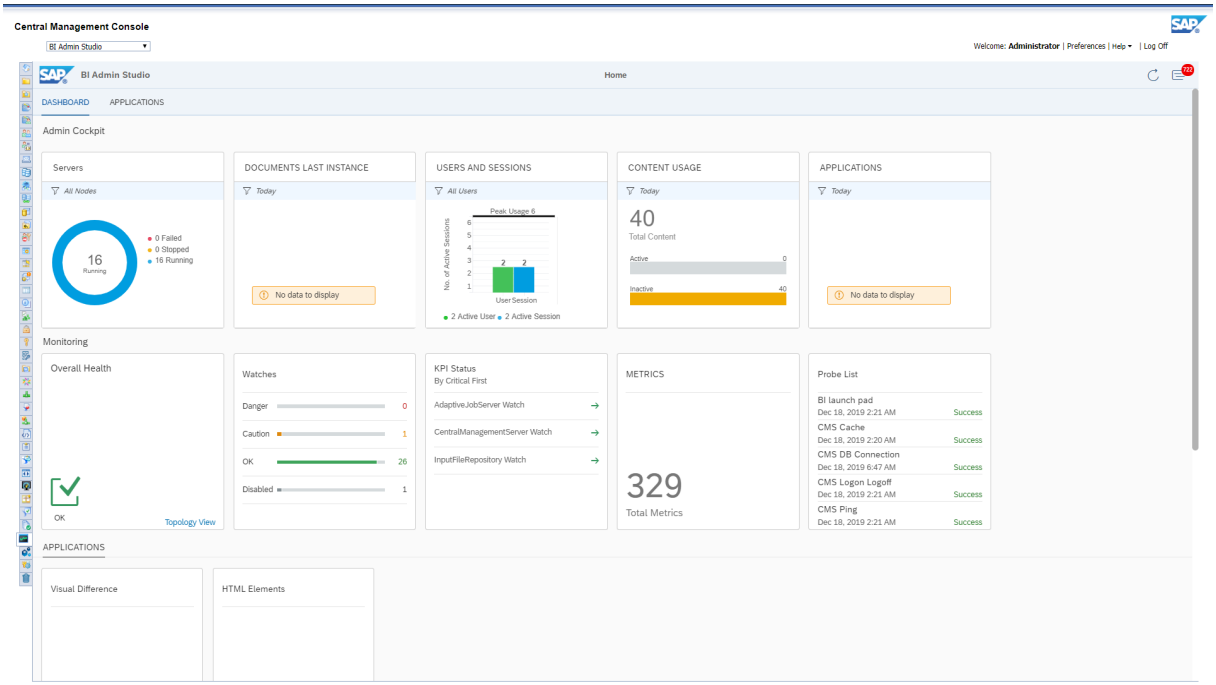
Procedure

1. In the *Universes* area of the CMC, select a universe in the list.
2. Click *Manage* > *Delete*.
3. When prompted for confirmation, click *OK*.

19 BI Admin Studio

BI Admin Studio is an application in CMC that combines Monitoring, Alerting, and Admin Cockpit, earlier known as BI Administrator's Cockpit.

The application comprises of two tabs *Dashboard* and *Applications*.



Dashboard

Dashboard tab provides a single-view of the dashboards that are available in *Admin Cockpit* and *Monitoring*. You can click on each dashboard to get detailed information about it. For example, you can select the *Servers* dashboard to get the list of servers, which have *Status* as *Running*, *Stopped*, and *Failed*, along with their details such as *Server Name*, *PID*, and *Type*. For more information on Admin Cockpit, refer to Admin Cockpit [page 723] and to learn more about Monitoring, refer to Monitoring [page 727].

Applications

You can access *Visual Difference* and *Authorized HTML Elements* from the *Applications* tab. For more information on *Visual Difference*, refer to Visual Difference [page 751] and to learn more about *HTML Elements*, refer to Authorizing HTML elements [page 753].

Alerting

You can select to access the notification pane for alerts. From the notification pane, you can select the option *To Alerts Page* to know more about the alerts that you have created.

19.1 Admin Cockpit

The Admin Cockpit is a new application added in the CMC. It enables an administrator to collect basic data about the BI environment. It means deriving business intelligence from within the data in your business intelligence environment. You can obtain information about Servers, Scheduled Jobs, Users and Sessions, Content Usage, and Applications with the Admin Cockpit.

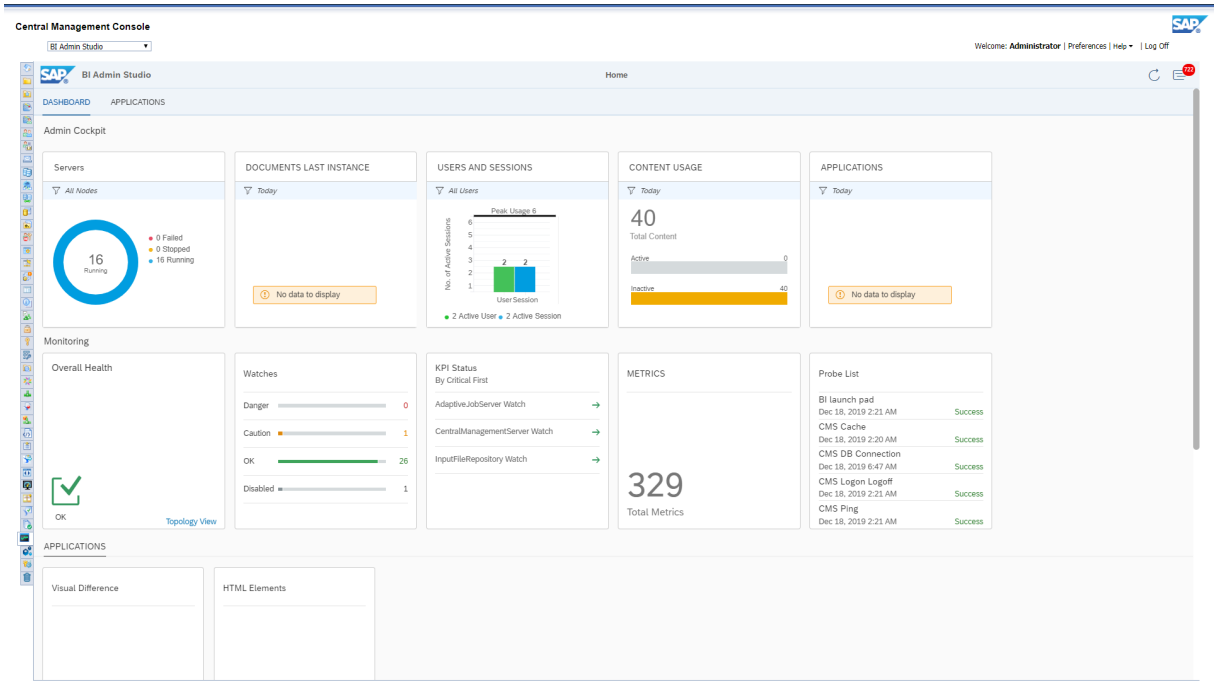
> **Note**
>
> The following requirements are necessary to ensure that the Admin Cockpit can be used successfully:
>
> - Monitoring service must be enabled.
> - Audit and relevant event must be enabled so that correct data is fetched.
> - - If you are not using internal RESTful Webservices (set the flag `use.boe.internal.biprws` in `...\webapps\BOE\WEB-INF\internal\Global.properties` to false), then:
>   1. Application server where the BI Platform RESTful Web Services are deployed must be up and running.
>   2. BI platform RESTful Web Service must be accessible by clients.
>   3. If you configure SSL for CMC, make sure to also configure SSL for application server where the BI Platform RESTful Web Service is deployed.
>   4. Access to cross domain must be enabled.
>
>   .
> - Users must belong to the Administrators group or any sub-group of it to access the Admin Cockpit.

19.1.1 Admin Cockpit

The Admin Cockpit gives you a comprehensive analysis of data related to the following components in a pictorial visualization:

- Servers
- Documents Last Instance
- Users and Sessions
- Content Usage
- Application

> **Note**
>
> Audit database must be enabled in order to view the analysis on *Content Usage* and *Application*.



You can refresh the data that appears on each page within the Admin Cockpit by clicking on the top-right corner of the Home Page.

19.1.2 BI on Servers

Admin Cockpit helps you obtain real-time data about the status and related details of all the servers in your BI environment.

The home page provides you with the following details:

- Total number of servers
- Number of servers with errors
- Number of stopped servers

You can filter data that appears on the *Servers* tile by selecting the desired server-cluster.

On clicking the *Servers* tile, you are directed to a Servers page that has the details of the total number of servers, the servers producing errors, and the stopped servers. The Servers page also provides you with the *Status*, *Server Name*, *PID* (process identifier), *Type*, *State*, and *Last modified time* for each error producing server.

Within the *Servers* page, you can filter data according to specific server-clusters by selecting the desired server cluster.

You can view more details about the error producing server by choosing the corresponding row. This directs you to a new page which details the reason for the error. You can restart the error producing server from within the page by choosing *START*.

19.1.3 BI on Document Instances

You can use the Admin Cockpit to obtain data on the status and related details for all instances of scheduled documents in your BI environment.

The Home Page gives you the following information:

- Total number of each scheduled document's last instance.
- Number of each scheduled document's last running instance.
- Number of each scheduled document's last error producing instance.
- Number of each scheduled document's last pending instance.

In the *Documents Last Instance* tile, you can filter data for a specific time range by selecting the desired time range from the drop-down menu. The available time ranges are:

- Today
- Last 7 days
- Last 30 days
- Quarter
- Year

When you click the *Documents Last Instance* tile, you are directed to the Last Instances page that has the details of the total number of each scheduled document's last instance, broken down by state: Running, Error, and Pending. The *Statistics* tab provides you details that you can view in the sections *Documents with most instances* and *Instances with longest run time*. The Documents Instances page also provides you with the *Instance Name*, *Status*, *Type*, *Owner*, and *End Time* for each error status.

You can export the data seen on the *Last Instances* page as a .CSV file by clicking the Export link button. You can also export selected instances by selecting its checkbox, and then *Export Selected* from the Export drop-down list.

You can view more details about an error producing instance by choosing the corresponding row. You can restart the job from within the page by choosing *RUN*.

In the statistics tab, new chart filter is enabled that allows you to filter and view the Top 5, Top 10, Top 15, and Top 20 documents.

19.1.4 BI on Users and Sessions

Admin Cockpit helps you obtain data about Users and Sessions in your BI environment.

For instance, the home page provides you with the following details:

- Number of active users
- Number of active sessions

In the *Users and Sessions* tile, you can filter data for:

- All users
- Named users
- Concurrent users

On clicking the *Users and Sessions* tile, you are directed to a Users and Sessions page that has the details of All Users, Top Users, and Statistics. The Statistics tab provides you with details related to Most Active Users and Most Inactive Users.

The Users and Sessions page also provides you with the *User Name*, *Total Sessions*, *Last Logon Time*, and *Longest Running Session*.

You can view more details about a particular user by choosing the corresponding row. This directs you to a new page which details the top sessions of that particular user. You can end any session of that particular user from within the page by selecting the desired session and choosing *END SESSION*.

19.1.5 BI on Content Usage

Admin Cockpit helps you obtain data about Content Usage in your BI environment.

For instance, the home page provides you with the following details:

- Number of active documents
- Number of inactive documents

In the *Content Usage* tile, you can filter data for a specific time range by selecting the desired time range from the drop-down menu.

> **Note**
>
> If you have deleted some active content, and filter data for a specific time range, the deleted item is still listed under active content, if it was active during the selected time range.

The available time ranges are:

- Today
- Last 7 days
- Last 30 days
- Quarter
- Year

On clicking the *Content Usage* tile, you are directed to a Content Usage page that has the details of the Active Content, Inactive Content, and Statistics. The Statistics tab provides you with details related to Inboxes with most Inactive Content, Universes with most content, and Folders with most content.

You can export the data seen on the *Content Usage* page in a csv file by choosing the export link button. You can also choose to export selected jobs by selecting the corresponding checkbox, and selecting *Export Selected* from the export drop-down.

The Content Usage page also provides you with the *Content Name*, *Type*, and *Run Time*.

In the statistics tab, new chart filter is enabled that allows you to filter and view the Top 5, Top 10, Top 15, and Top 20 documents.

19.1.6 BI on Applications

Admin Cockpit provides you with data about the number of applications sorted by the application name in your BI environment.

In the *Application* tile, you can filter data for a specific time range by selecting the desired time range from the drop-down menu. The available time ranges are:

- Today
- Last 7 days
- Last 30 days
- Quarter
- Year

On clicking the *Applications* tile, you are directed to an Applications page that has the details related to *All Applications* and *Top Applications*.

The *Top Applications* tab lists the top 5 applications with the most number of documents created in the selected time range. The Applications page also provides you with the *Application Name*, *No. of users*, and *No. of artifacts*.

19.2 Monitoring

The Monitoring application allows you to capture the runtime and historical metrics of BI platform servers, for reporting and notification. The monitoring application helps system administrators to identify whether an application is functioning normally and if the response times are as expected. By providing key business metrics, the monitoring application provides better insight into the BI platform.

Monitoring allows you to perform these tasks:

- Check the performance of each server: This is possible with the help of watches, which show the state of each server as traffic lights. The system administrator can set thresholds for these watches and receive alerts when these thresholds are breached, and help take an action in case of failure or outage.
- View critical system Key Performance Indicators (KPIs): This helps in activity and resource monitoring. These KPIs are displayed on the dashboard page of the monitoring application.
- View the entire BI platform deployment (both in graphical and tabular format) based on Server Groups, Service Categories, and Enterprise Nodes.
- View the recent failures on the dashboard screen.
- Check system availability and response time: Using probes, you can simulate workflows to check if the servers and services in the BI platform deployment are functioning as expected. By analyzing the round-trip time of these probes at periodic intervals, the system administrator can assess the system usage pattern.
- Analyze peak load and peak period for the CMS: This helps the system administrator determine if more licenses or system resources are required.
- Integrate with other enterprise applications: The BI platform monitoring application can be integrated with other enterprise applications like SAP Solution Manager and IBM Tivoli Monitoring.

- Track the *Auditing Level* metric value under *Central Management Server* when the *Set Events* is selected as *Off* (metric value 1). A watchlist can be created here, when the metric value is 1, a test alert is sent in the watchlist along with an email alert.

For more information about using the monitoring application, including details about probes and watches, see the *SAP BusinessObjects Business Intelligence platform CMC Online Help*.

Related Information

About the Server Metrics Appendix [page 1085]

19.2.1 Monitoring terms

The following list provides terms that relate to the monitoring application:

Trend

To record or display historical data for the purpose of finding trends.

Dashboard

The Dashboard page provides a centralized view for the system administrator to monitor the performance of all servers. It provides real-time information on the system KPIs, recent alerts, and watches, and corresponding graphs based on the watch states.

Watch

Watches provide real-time status and historical trends of servers and workflows within the BI platform environment. Users can associate thresholds and alerts with watches. You can create a watch using data from probes, servers, SAPOSCOL, or derived metrics.

Derived metric

Derived metrics are metrics that you create by combining two or more existing metrics in a mathematical equation. You can create a metric based on the user's requirements, and then create a watch using this metric.

Topological metric

Topological metrics provide you with the net state for each service category in the BI platform. For example, the Crystal Reports service gives you the combined health state of all the watches related to Crystal Reports servers.

Health State

These are the health state values:

- "0" - "DANGER"
- "1" - "AMBER"
- "2" - "GREEN"

KPI

KPIs (key performance indicators) are standard metrics in the BI platform. They provide information about schedules and login sessions. For example, a higher number of *RunningJobs* indicates good performance of the servers. Alternatively, a higher number of *PendingJobs* indicates poor performance and high system load.

Probe

Probes monitor different services and simulate the different functionalities of the BI platform components. By scheduling probes to run at specified intervals, the system administrator can track the availability and performance of key services provided by the BI platform. This data can also be used for capacity planning.

Traffic light

A traffic light is an icon that displays the color Green, Amber, or Red to indicate the state of a watch at any given time. Users can choose to set two or three states to a watch.

Trending graph

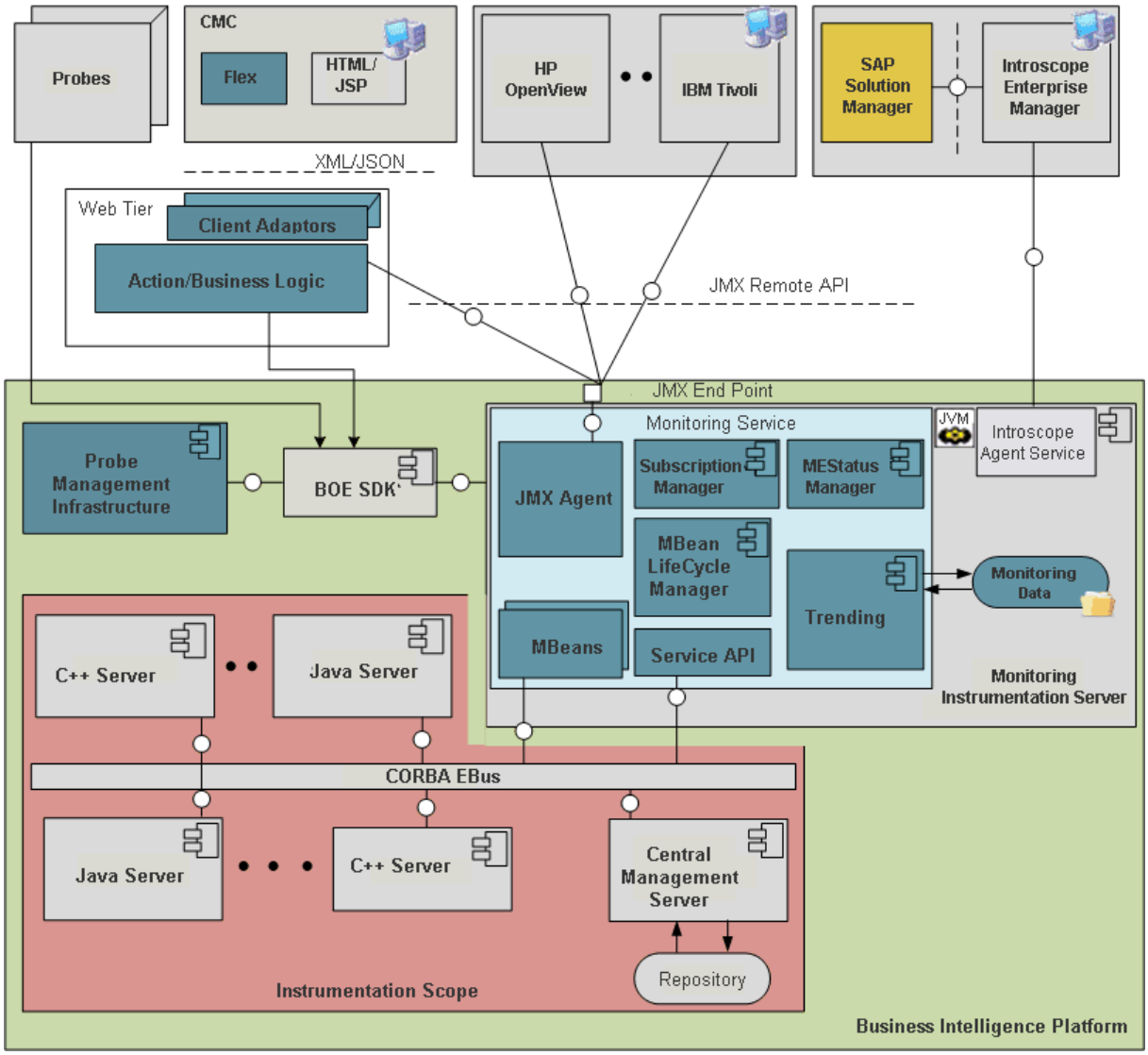
A trending graph is a graphical representation of historical metric data generated by probes and servers. It helps the system administrator monitor the system at different time intervals, and assess the system usage pattern.

Alert

An alert is a notification generated by the monitoring application, when a user-defined threshold value set for different metrics applied to a watch is breached. You can choose to receive alerts either through email or on the *Dashboard* page.

19.2.1.1 Architecture

This section provides a high-level overview of the monitoring architecture and briefly explains the roles the components play. The monitoring architecture is represented graphically below:



The high-level components in the architecture are listed below:

- The Adaptive Processing Server (APS)

- The Java Management Extensions (JMX) agent/server
- MBeans
- JMX Clients
- The Management consoles
- Trending Database

The monitoring service is hosted on the Adaptive Processing Server. The application is based on JMX technology.

The Monitoring Service provides the core services available in the monitoring application. The Monitoring Service provides the following services:

- Provides the JMX agent service.
- Creates MBeans dynamically for the SAP BusinessObjects servers.
- Provides lifecycle management for the MBeans.
- Provides a mechanism for registering new probes.
- Allows users to create complex threshold conditions using the metrics of the servers.
- Provides a threshold notification mechanism and sends alerts.
- Stores historical data.

The Probe Scheduling Service that is hosted on the Adaptive Job Server manages the running and scheduling of probes. Hence, the Adaptive Job Server should be running for the probes to run.

The monitoring application also exposes a JMX or Remote Method Invocation (RMI) URL end point. Other enterprise applications such as IBM Tivoli Monitoring can connect to the monitoring application and access the BI platform metrics by using a JMX Remote API. The monitoring application uses the Auditing Data Store (ADS) database for storing historical data for the purpose of trending. For information on the trending database schema, see Trending database schema [page 1119].

19.2.2 Configuring database support for Monitoring

This section describes how to set up monitoring, and report against monitoring data.

> **Note**
>
> Only watches that have the setting *Write to Trending Database* selected write monitoring information to the trending database.

There are two database options for recording monitoring information: either record information using the Auditing Data Store (ADS), or any other database supported by the platform using JDBC driver.

> **Note**
>
> Apache Derby database is deprecated in BI 4.3 release. For more information on migrating and backing-up data, refer to 2912759.

You can use the default Auditing Data Store (ADS), often referred to as the auditing database. This is the relational database where the CMS stores auditing data. You can use either ADS included with the BI platform, or any other supported database that you've configured as your auditing database.

Other supported databases are:

- DB2
- SQL Server
- My SQL
- Oracle
- SAP HANA Database
- SQL Anywhere
- Sybase

Using the auditing database allows users to report from the auditing data together with the monitoring information. Capturing the data in a relational database provides backup and recovery capability, and the real-time availability of data.

Related Information

Configuration for using the auditing database [page 732]

19.2.2.1 Configuration for using the auditing database

If you want to use the auditing database for your monitoring data, you will need to perform extra configuration steps as follows:

- Prior to BI 4.3, if you had data in your Derby trending database, then you will have to migrate the Derby database to the auditing database, and then configure the BI platform to record monitoring information in the auditing database. These are the high-level steps you'll need to follow. For details, see the related topics.
  1. Migrate the Derby database.
  2. Configure the SBO files and add alias names.
  3. Switch to the auditing database.
  4. Restart the Adaptive Processing Server that hosts the Monitoring Service.
  5. On the Monitoring Dashboard, ensure that everything works as expected. Verify that these monitoring tables have been created in the database:

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- If you do not have data in your trending database, that is, you have a fresh installation, you do not need to migrate the database; you only need to configure the BI platform to record monitoring information in the auditing database. These are the high-level steps you'll need to follow. For details, see the related topics.
  1. Verify that the auditing database is working, and auditing is running properly.
  2. Create the monitoring tables in the ADS.
  3. Configure the SBO files and add alias names.

4. Switch to the auditing database.
5. Restart the Adaptive Processing Server that hosts the Monitoring Service.
6. On the Monitoring Dashboard, ensure that everything works as expected. Verify that these monitoring tables have been created in the database:

   MOT_MES_DETAILS
   MOT_MES_METRICS
   MOT_TREND_DATA
   MOT_TREND_DETAILS

> **Note**
>
> If you record Monitoring data to the auditing database, and you want to report from this data, you will need to develop a custom universe.

Related Information

Configuring SBO files [page 735]
Adding alias names in the SBO file [page 737]
To switch to the auditing database [page 738]
To create the monitoring tables in the ADS [page 733]

19.2.2.1.1 To create the monitoring tables in the ADS

Context

Follow these steps to prepare the target auditing database:

Procedure

1. After installing the BI platform, DDLs related to all the supported CMS auditing databases are available in the `<Install Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` location. You will find seven different (.sql extension) files with the respective database name. For example: `Oracle.sql` for Oracle, `Sybase ASE.sql` for Sybase ASE Database, and so on.
2. Go to the target database (in this case, the target database is the database where CMS auditing has been configured) and run the .sql file. The following four Monitoring tables are created: `MOT_TREND_DETAILS`, `MOT_TREND_DATA`, `MOT_MES_DETAILS`, and `MOT_MES_METRICS`. The required indexes are also created, along with the tables.

Results

If all the tables are created with correct data types as mentioned in the .sql file, the database schema required for the Monitoring application is created.

19.2.2.1.2 To restore contents to the target database

Context

The following steps need to be performed in order to restore the content to the target database:

Procedure

1. Enable Identity Insert.

   The Monitoring tables contain a number of IDENTITY columns. These are columns that auto-generate their values. Certain databases (for example MS SQL Server and Sybase ASE) do not allow explicit insertion of values to these columns. During data migration, even these identity column values need to be migrated however. Users therefore have to enable the explicit insertion of these values using the following SQL command: `SET IDENTITY_INSERT <TABLE NAME> ON`.
2. Import the CSV dump file to the target table.

   All software provided by database clients enables users to import the data from CSV to the table using either a menu option or a command. The user needs to use this option to import the data from the CSV file to the corresponding table. Import the data files into the new tables in the following order:
   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `MOT_MES_METRICS`
3. Disable Identity Insert.

   Once the data has been imported, the user needs to disable the identity insert on the table using the following SQL command: `SET IDENTITY_INSERT <TABLE NAME> OFF`.

   Users have to disable the identity insert on a table after the data import in order to enable the identity insert on the next table. This is because the identity insert operation can be enabled on only one table at a time.

Results

Enabling or disabling Identity Insert applies only to MS SQL Server and Sybase ASE. For other databases such as Oracle, MaxDb, DB2, MySQL, or SQL Anywhere, this is not required. You can import the data to the tables directly.

19.2.2.1.3 Configuring SBO files

Internally, the Monitoring application uses Connection Server libraries, and the SBO configuration is required for the Connection Server to establish connectivity to the database driver. You need to specify the database driver and its location in the SBO file to establish this connectivity.

> **Note**
>
> The Monitoring application refers to the auditing connection name, and uses JDBC if `<hostName>.<Portnum>.<dbName>` is used, or ODBC otherwise. The Connection Server SBO files need to be configured accordingly for the Monitoring application to be able to connect to the auditing database.

> **Note**
>
> For Oracle databases, only JDBC connections are supported.

Example

- If the Connection name field configured in the CMC Auditing page is `<hostName>.<Portnum>.<dbName>`, the driver JAR should be configured in: `dataAccess\connectionServer\jdbc\<dbType>.sbo`.
- If the Connection name field configured in the CMC Auditing page is an ODBC DSN, the driver should be configured in: `<Install_Dir>\dataAccess\connectionServer\odbc\<dbType>.sbo`.
- If the database used for auditing is SAP HANA, the file where the driver needs to be configured is: `<Install_Dir>\dataAccess\connectionServer\odbc\newdb.sbo`.
- If the database used for auditing is MS SQL Server, the file where the driver needs to be configured is: `<Install_Dir>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- If the database used for auditing is DB2 server, the connection server does not contain a supporting `db2iseries.sbo` file.
  By default, the monitoring application uses the ODBC connection mode to connect to the DB2 auditing database. To work in this mode, you must add and configure the System DSN (for the DB2 server) in the machine on which monitoring application is running. For information on how to add and configure the ODBC connection for DB2, refer the following links:
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024166.htm
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024200.htm

  > **Note**
  >
  > If you do not configure the System DSN for DB2, the monitoring trending fails.

Configuring SBO files

Typically, the ODBC libraries are already configured in the SBO files and you just need to add the alias names. If this is not the case, follow these examples to perform the configuration in the SBO file:

Example

- If the database version used for auditing is SAP HANA, the configuration in SBO should be:

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
    <Aliases>
        <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
        <Alias>Hana</Alias>
    </Aliases>
    <Libraries>
        <Library Platform="MSWindows">dbd_wnewdb</Library>
        <Library Platform="MSWindows">dbd_newdb</Library>
    </Libraries>
    <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- If the database version used for auditing is MS SQL Server 2008, the configuration in SBO should be:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
    <Libraries>
        <Library>dbd_wmssql</Library>
        <Library>dbd_mssql</Library>
    </Libraries>
    <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
    <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
    <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
    <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- id="li_9D4EB94F9752458BB21A940C0A892C6D">If the database version used for auditing is MySQL 5, the SBO should have this entry:

```
<DataBase Active="Yes" Name="MySQL 5">
    <JDBCDriver>
        <ClassPath>
            <Path>C:\mysqljdbcdriver.jar</Path>
              </ClassPath>
        <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
        <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</
Parameter>
    </JDBCDriver>
    <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
    <Parameter Name="Force Execute">Always</Parameter>
    <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

- If the database version used for auditing is Oracle, the configuration in SBO should be:

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>
```

```
<Path>C:\app\Administrator\product\11.2.0\client_64\jdbc\lib\ojdbc6.jar</Path>
            </ClassPath>
               <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
               <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
       </JDBCDriver>
       <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
        <Parameter Name="Escape Character">/</Parameter>
         <Parameter Name="Force Execute">Always</Parameter>
         <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

For more information on configuring the driver in SBO files, refer to the *Data Access Guide*.

19.2.2.1.4 Adding alias names in the SBO file

In addition to configuring the driver, users also need to add an alias in the SBO, under the database version that is being used for auditing. The following table lists the alias names that should be used for specified databases.

DB Name	Alias Name to be used in SBO
SAP HANA	Hana
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

You need to use the specified names, as the Monitoring application searches the SBO for these names.

Example

If the database used for auditing is MS SQL Server 2008, the alias needs to be added to the SBO as shown:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</
Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
```

```
    </DataBase>
```

19.2.2.1.5 To switch to the auditing database

Context

Switch the database so that Monitoring trending information will be stored in the auditing database.

Procedure

1. In the *Manage* area on the CMC home page, click *Applications*.
2. Click *BI Admin Studio*.
3. Then click *Monitoring properties.*
4. Double-click *Monitoring Application* to open the properties page.
5. In the *Trending Database Settings* area, select *Use Audit Database*.

Next Steps

> **Note**
>
> If you are using an Oracle database for auditing, the *ADS Database Connection Name* on the Auditing page in the CMC needs to be specified as a JDBC connection. Specify the connection name as follows: `<server_name>,<port>,<service_name>`.

> **Note**
>
> To ensure that the monitoring tables are created correctly, grant the following permissions for the database user account:
>
> EXECUTE
> CREATE SEQUENCE
> CREATE TRIGGER

19.2.2.2 Configuring Monitoring Database using JDBC

Prerequisites

You have created a JDBC connection. To create a new JDBC connection, perform the following steps.

1. Place the JDBC driver jar for the database that you want to configure in the following location: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\MON.MonitoringService\lib>`.

   > **Note**
   >
   > In clustered depolyments, you should copy the JDBC driver to the system that hosts monitoring services.

2. Restart SIA.

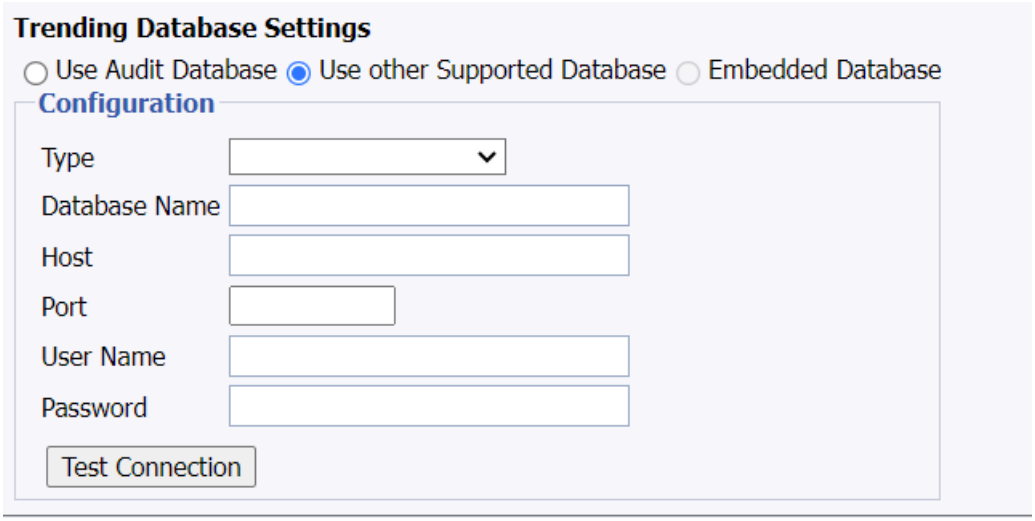
Context

To configure a new database for BI Monitoring, proceed as follows:

Procedure

1. Log on to the CMC.
2. On the CMC home page, select *Applications* from the dropdown menu.
3. Righ-click *BI Admin Studio* and select *Monitoring Properties*.

   The *Monitoring Application Properties* popup window appears. By default, the *Use Audit Database* radio button is selected.
4. Select the *Use other supported database* radio button.
5. Enter the *Type*, *Database Name*, *Host*, *Port*, *User Name*, and *Password*.



6. **Optional:** Add a number of days after which the platform should delete the monitoring history data using the *Delete all history older than X days* property.
7. Choose *Save & Close*.
8. Restart Adaptive Processing Server.

   You may validate your connection by choosing *Test Connection*.

> ⓘ Note
>
> You need to restart all APS servers that host BI Monitoring service for the changes to take effect.

Results

You have now configured a new database to store comments from the BI Monitoring application.

19.2.3 Configuration properties

This section describes the monitoring application properties and how you can edit them.

To see the configuration properties of the monitoring application:

1. On the CMC home page, click *Application*.
2. Right-click *BI Admin Studio* and select *Monitoring Properties*. The configurable properties are described in the below.

Section	Field	Description
	Enable Monitoring Application	Select this option to enable monitoring functionality. If you deselect this option, all monitoring functions except probes will be disabled. Probe trending will also be disabled.
	Default JMX agent end point URL (IIOP)	This contains the default JMX agent end point URL that uses the IIOP protocol. This URL is generated automatically if you enable monitoring and then restart the server. This is the default protocol for the monitoring service. This is a read-only field.

Section	Field	Description
RMI	*Enable RMI protocol for JMX*	By default, this option is disabled. If you enable this option, you must provide the RMI port number. This port will be used for both RMI registry entry and RMI connector port. This port should be available for the service; otherwise the service will fail to start. After you provide the RMI port number, restart the server. Once the server is restarted, the RMI JMX agent end point URL is generated. This is a read-only property containing the JMX agent's end point URL using the RMI protocol. Use this URL to connect to monitoring from other clients.
Host Metrics	*Enable host metrics*	By default, this option is disabled. If you enable this option, you must provide the path to your installation of the SAPOSCOL binary To enable host metrics, you need to install SAPOSCOL. For more information on how to install SAPOSCOL, see “Installing SAPOSCOL”.
Trending Database Settings	*Use Audit Database*	Select this option to store the trend history of metrics in the Auditing Data Store (ADS) auditing database. **Note** Auditing Data Store has to be configured for this to work.
	Use Other Supported Database	Select this option to store the metric/watch trend history in a supported database that you have configured.
	Delete all history older than X days	Specifies how long, in days, the history data should be kept.
Other settings	*Metric Refresh Interval (seconds)*	The minimum interval that you can specify is 15 seconds. This interval governs the following: • Subscription computation of the watches: The caution and danger rules are computed continuously with the specified time interval. • Calculating the watch state: Watch states are computed continuously with the specified time interval if the Event setting of the watch is selected with the following option: *Change the watch state every time caution or danger evaluates to true*. • Trending period: History mode for the graphs is recorded continuously with the specified time interval.

Section	Field	Description
	Monitoring UI auto refresh interval (seconds)	This interval will be used in the monitoring user interface (including the dashboard, watch list, and probes) for auto refresh. The minimum interval is 15 seconds. Auto-refresh does not affect the time duration in Live mode in graphs, which is set to 15 seconds by default.
	Alert Reminder Frequency (days)	Specifies the number of days before an alert reminder is generated.

3. Click *Save*.

> **Note**
>
> When you change any of these properties except enabling and disabling the monitoring application, you must restart the Adaptive Processing Servers that host the monitoring services.

Installing SAPOSCOL

Perform the following steps to install SAPOSCOL:

1. Download `SAPHOSTAGENT710_XX.SAR` from SAP Marketplace (http://service.sap.com).
2. Extract `SAPHOSTAGENT710_XX.SAR` by executing the `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR` command.
3. Install `saphostexec` by executing the `saphostexec.exe -install` command. Once saphostexec is installed as a service, SAPOSCOL is started.
4. Check SAPOSCOL status by executing the `saposcol -s` command.

19.2.3.1 JMX end point URL

The monitoring application exposes a JMX end point URL through which other clients can connect using JMX Remote API. By default, the JMX connectivity is provided over the IIOP (Internet Inter-Orb Protocol) or CORBA (Common Object Request Broker Architecture) transport. This connection URL is displayed in the properties page of the monitoring application. Being able to connect over IIOP absolves the need to worry about firewalls and having to expose ports. The CORBA ports are available by default. The jar files listed in the following table are needed at the JMX client end to be able to connect:

Jar Files
`activation-1.1.jar`
`axiom-api-1.2.5.jar`
`axiom-impl-1.2.5.jar`
`axis2-adb-1.3.jar`

Jar Files
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

Another option is to connect through the default RMI port. For more information on how to connect through the RMI port, see Configuration properties [page 740].

19.2.3.2 JMX SSL Configuration

You can now accomplish secure communication between JConsole and BOE through JMX SSL configuration.

Procedure

1. Login to CMC.
2. Navigate to *Applications* > *BI Admin Studio* > *Monitoring Properties*.
3. Under *RMI*, enable the *Enable RMI protocol for JMX* option.
4. Enter the RMI port number.

   7777
5. Enable the *Enable SSL for RMI protocol for JMX* option.

6. Click *Save* and *Close*.
7. Restart the *Adaptive Processing Server*.

> **Note**
>
> The server hosting the monitoring service is restarted.

19.2.3.2.1 Generate Certificate

Procedure

1. Open the command prompt in Administrator mode or a terminal session, and navigate to this location:

   Windows:

   `INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`

   Linux / Unix:

   `INSTALLDIR/sap_bobj/enterprise_xi40/<PLATFORM>_x64/sapjvm/bin`
2. Execute the command to generate a certificate: `keytool -genkeypair -alias serverkey -keyalg RSA -keysize 2048 -keystore serverkeystore`
3. Enter all the required information for creating a certificate.
4. 4. Once the execution is successful, it creates a certificate file by name in the same sapjvm bin directory: `serverkeystore`

19.2.3.2.2 Adding a Certificate Store file to Monitoring Service

Procedure

1. In CMC, navigate to *Servers* > *Servers List*.
2. Select *Adaptive Processing Server* (Server Hosting Montoring Service).
3. Select *Properties*.
4. Navigate to the *JMX SSL Configuration* section.
5. In the *Certificate Store File Location*, enter the path of the *Certificate Keystore file location*.
6. Enter the *Private Key Access Password* information.

   Password1

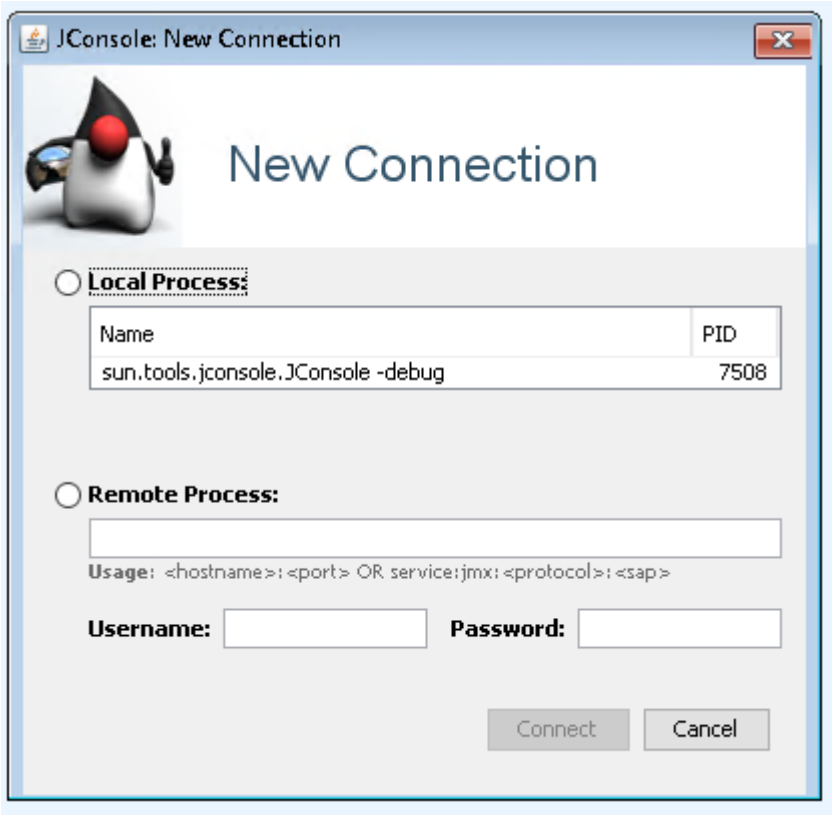
19.2.3.2.3 Connecting to JConsole

Procedure

1. Execute the command to launch `JCONSOLE.exe` in the command prompt (`jconsole.exe -J-Djavax.net.ssl.trustStore="<Path of Certificate Keystore file location >" -J-Djavax.net.ssl.trustStorePassword=<PasswordDetail>`)

   ```
   jconsole.exe -J-Djavax.net.ssl.trustStore="C:\Program Files
   (x86)\SAP BusinessObjects\SAP BusinessObjects
   Enterprise XI 4.0\win64_x64\sapjvm\bin\serverkeystore" -J-
   Djavax.net.ssl.trustStorePassword=Password1
   ```

2. Once the above command is executed, it launches the JConsole Viewer as shown below.



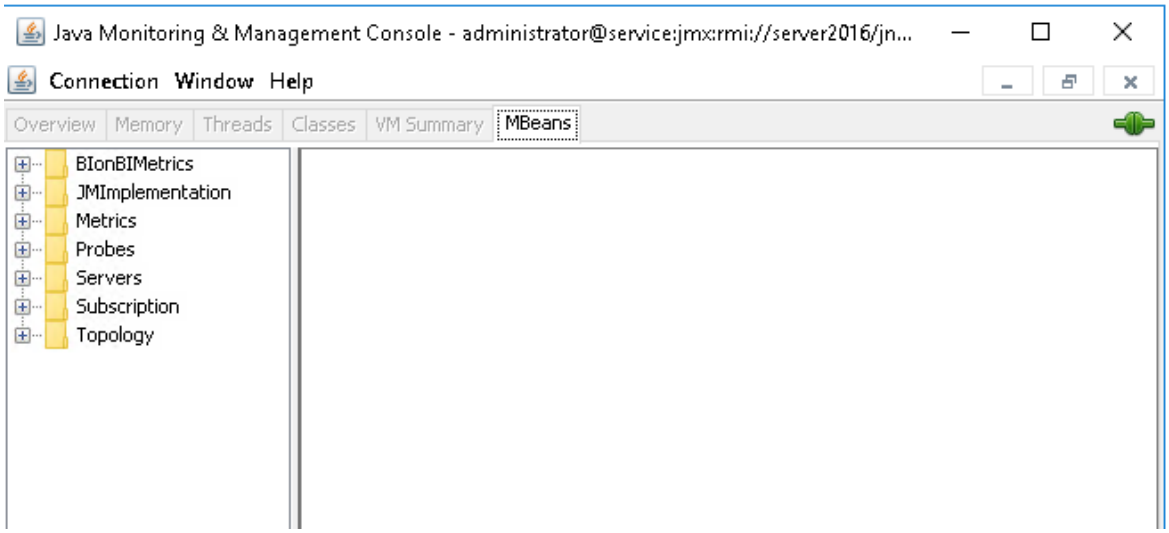
3. Click the *Remote Process* radio button to enable the field.
4. Enter the *RMI JMX agent end point URL*, and the associated *Username* and *Password*.

   The *RMI JMX agent end point URL* format is: `service:jmx:rmi://<HostName>/jndi/rmi://<HostName>:<RMI Port Number>/<hostname>:<CMS Port>`.

   `service:jmx:rmi://server2016/jndi/rmi://server2016:7777/server2016:6400`.

5. Click *Connect*.

6. The JConsole viewer *JAVA Monitoring & Management Console* is launched.



7. In the JConsole viewer, you can navigate to different sections such as BIonBIMetrics, Metrics, Probes, Servers, and Topology to retrieve the related data.

19.2.3.3 HTTPS authentication for monitoring probes

HTTPS server authentication for monitoring probes is supported, and requires the following configuration prior to use:

1. Import the server certificate into the client's truststore. This allows the client side (the probe) to verify the server's identity. Run this command: `<INSTALL_ROOT>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore "<INSTALL_ROOT>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" –file ca.cer`
`ca.cer` is either the server's self-signed certificate, or the certificate of the Certificate Authority (usually an internal CA) that generated the server's certificate. If the server's certificate is generated by a well known CA, then there is no need to import it, and this step can be skipped. This is because the server's certificate will be verified with the CA, whose public key is already in the truststore by default.
2. Change the *URL base* in the BI launch pad probe's settings to `https://<URL>/BOE/BI`, where <URL> refers to the host by the name used in the certificate.

HTTPS client authentication for monitoring probes is not supported.

19.2.3.4 Password encryption for probes

When using probes, to ensure that passwords are encrypted, you must add the `true` parameter to every monitoring probe's password parameter when you create the probe through the command line. For more information and a syntax example, see the topic *Managing Probes Through the Command Line* in the CMC help.

19.2.4 Integrating with other applications

Enterprise solutions, such as IBM Tivoli Monitoring, integrate with the monitoring application as JMX clients connecting via the JMX end point URL. After integration, the SAP BusinessObjects metrics can be viewed from the client's user interface.

19.2.4.1 Integrating the monitoring application with SAP Solution Manager

To integrate the monitoring application with SAP Solution Manager, you need to have Wily Introscope installed and running in your system. The SAP Solution Manager must be configured for Introscope workstation. Perform the following steps during BI platform installation:

1. In the "Configure Connectivity to Wily Introscope Enterprise Manager" step, provide the host name and port details. An Introscope Agent will be installed at `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wily` when the BI platform is installed.
2. Launch the Wily Introscope workstation, and click *New Investigator*. You can view the SAP BusinessObjects server metrics and probe virtual metrics in the JMX section of the agent configured.

> **Note**
>
> You can configure the Wily Introscope (IS) agent by choosing *CMC* > *Servers* > *Server node* > *Placeholders*. The IS Enterprise Manager host and port are also configured here for the IS agent to communicate with the monitoring application. For more information, see *Managing Servers* in the CMC help.
>
> For the JMX metrics to be available in IS, ensure that both the IS agent services and monitoring service are available on the AdaptiveProcessingServer Instance.
>
> If you enable IS instrumentation, the code instrumentation is enabled automatically.

19.2.5 Cluster support for monitoring server

The monitoring application supports clustering, which provides failover capability.

With cluster support, only one service is active at any given time, and all other services are passive. If there are two monitoring services s1 and s2 in a clustered environment, only one of them is available. Both s1 and s2 attempt to become active, but when one of them succeeds, the other service becomes inactive or passive.

The passive service checks the availability of the active service periodically (every minute). If the active service is unavailable, the passive service immediately attempts to become active.

> **Note**
>
> It is recommended that the monitoring service be hosted on a separate Adaptive Processing Server (APS) instance to avoid failures or poor performance of the APS.

19.2.6 Troubleshooting

This section provides step-by-step solutions to a wide range of problems that may occur in your work with the monitoring application.

19.2.6.1 Dashboard

Monitoring link is not displayed on the CMC page

- Check if the user has adequate access rights.
- Ensure that the user is added to the Monitoring User or Administrator groups or any other group which is a part of these groups.

Key Performance Indicators (KPIs) are not visible on the Monitoring Dashboard

- Check if the required metrics are visible by choosing *CMS Server properties* > *Metrics*.
- Ensure that the Central Management Server is responding as expected.

19.2.6.2 Alerts

Unable to receive alerts on the Alerts page

- Check if the *Enable My Alerts* option in the Alerting application properties is selected.
- Ensure that you have adequate access rights to receive alerts.
- Check if the recent alerts are visible on the monitoring dashboard.

> **Note**
>
> You can send a Crystal Reports document to the email ID you set to test if the SMTP is working as expected.

Unable to receive email notifications

- Check if the *Enable Email* option in the Alerting application properties is selected.
- Check if the email address settings for receiving email alerts is appropriate.

- Check if the SMTP server is functioning.
- Ensure that the Adaptive Job Server instance is enabled.
- Check the SMTP settings in the Adaptive Job Server instance destination.

19.2.6.3 Watchlist

Unable to receive historical data for Watch

- Check the polling interval on the monitoring application *Properties* page.
- Check the trace file in the logging folder.
- Check if the system time of the server and client is the same in a specific time zone.

An error occurred while retrieving synchronized live data

Check if the Adaptive Processing Server instance is running.

Watchlist tab is disabled

- Check if the Monitoring service is running.
- Check the monitoring service logs for error messages.
- Check if the servers and their metrics are visible in jConsole.

19.2.6.4 Probes

Unable to schedule Probes

- Check if the AdaptiveJobServer instance that hosts the Probe Scheduling Service is running.
- Ensure that the report CUID, that is used for Crystal Reports and Web Intelligence documents, is appropriate.
- Ensure that the user has administrative rights or is a member of the Administrator group.
- Check if the user has adequate rights to open, refresh, export Crystal Reports or Web Intelligence documents that are used in the corresponding probes.

Probe schedule status is pending

- Check if the ProbeSchedulingService instance is installed.
- Check if the AdaptiveJobServer instance that hosts the Probe Scheduling Service is running.

An error occurred while retrieving the trend data from the database

Check if the AdaptiveProcessingServer instance is running.

probeRun.bat fails to run successfully

- Check if `java_home` is set.
- Check if the correct parameters are entered in the command prompt.

> **Note**
>
> Enter **`probeRun.bat -help`** in the command prompt to check if all the parameters are appropriate.

19.2.6.5 Metrics

Host metrics are not listed

- Ensure that SAPOSCOL is running.
- Ensure that the *Enable Host Metrics* option is selected on the monitoring application *Properties* page.
- Restart the AdaptiveProcessingServer instance for the changes to be effective.
- Ensure that *Path to your installation of SAPOSCOL binary* is appropriate.

Error occurred while retrieving JMX Client

Check if the AdaptiveProcessingServer instance is running.

SAPOSCOL metric value is zero on the Metric page

- Ensure that SAPOSCOL is running.

- Execute the following on the host where SAPOSCOL is installed:
  1. `saposcol -s` to check the status
  2. `saposcol -m` to get a snapshot of the data collected by SAPOSCOL

19.2.6.6 Graph

Graphs show different times for the live and history modes

Ensure that the system time of the server and client is the same in a specific time zone.

19.3 Visual Difference

Visual Difference allows you to view the differences between two versions of an LCMBIAR or an object or both. You can use this feature to determine the difference between files or objects to develop and maintain different report types. This feature gives a comparison status between the source and the destination versions. For example, if a previous version of the user report is accurate and the current version is inaccurate, you can compare and analyze the file to evaluate the issue.

Home Page

The visual difference home page consists of the following tabs and panes:

- New Comparison - this tab allows you to create new comparison between objects
- Search Comparisons - this field allows you to search for the already compared objects
- Comparisons pane - this pane lists the filters and differences tabs
- Comparisons: Differences pane - this pane lists the compared objects with the comparison name, Date/Time and the status of the differences

19.3.1 To compare objects or files using Visual Difference

Context

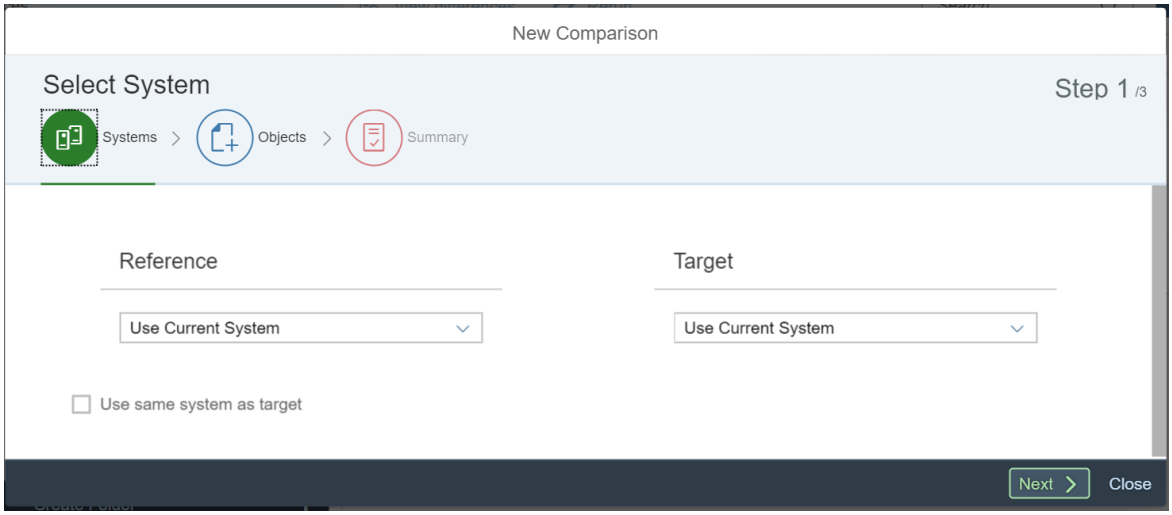
To compare files using visual difference, complete the following steps:

Procedure

1. Log into the CMC application.
2. In the CMC homepage, under the *Manage* tab, click the *Visual Difference* link.
   The Visual Difference page is displayed. The compared files are stored in the "Differences" folder, or in any of the user created sub-folders.

   > **Note**
   >
   > To create a new sub-folder, select the Create Folder +.

3. Select + to create a new comparison.
   The *New Comparison* wizard is displayed.



4. Select the *Reference* and *Target* system from the dropdown.
   You can connect to any of the following reference and target systems:

   > **Note**
   >
   > If an object is added in the Version Management System (VMS), then you will get the option to select versions in the next step.

   - CMS
   - Local File System

5. In the *Object Selection* screen, search and select the object or a file from the *Reference* and *Target* system.
6. Change the *Comparison Name*, if necessary.
7. Select *Compare* to compare the objects.

   > **Note**
   >
   > - You can check the differences by selecting the comparison first, and then *View Differences*. The differences are highlighted in orange color, and the missing objects are highlighted in red color.
   > - You can run the comparison again by selecting the comparison first, and then *Rerun*

   The comparison process starts immediately.

You can also use the filter option to view the compared objects by type, and with differences or with common attributes.

19.3.2 To compare objects or files using the Version Management System

You can compare promotion management jobs or folders in a version management system using the visual difference option.

To compare objects in a version management system, complete the following steps:

1. Log on to the CMC application.
2. In the CMC homepage, under the *Manage* tab, click the *Visual Difference* link.
   The Visual Difference page is displayed. The compared files are stored in the "Differences" folder, or in any of the user created sub-folders.

   > **Note**
   >
   > To create a new sub-folder, click the Folder icon.

3. Click *New Comparison*.
   The *Visual Difference - Comparisons* screen is displayed.
4. Select *Logon to VMS* from *Select System* under Reference.
5. Enter the login credentials to the VMS, and click *Log On*.
   The *Visual Difference - Auto Select Target System* dialog box is displayed
6. Click *No* if you want to set a different target system, or click *Yes* if you want to set the target system same as the reference system.
7. Click *Browse* to select the objects or jobs that you want to compare from both the reference and target systems.
8. Click *Add*.
   The objects selected for comparison are listed in the *New Comparison* pane.
   You can compare the files immediately, or schedule the comparison for a later point of time. To compare the files, continue with the next step.
9. Click *Compare* to compare jobs or folders.
   The comparison process starts immediately and the differences if any are displayed in the *Visual Difference viewer*. The differences are highlighted in orange color, and the missing objects are highlighted in red color.
   You can also use the filter option to view the compared objects by type, and with differences or with common attributes.
10. Click *Save* to save the difference report.
11. Specify the location where you want to save the report, and click *OK*.

19.4 Authorizing HTML elements

To let users benefit from the capabilities of trustworthy HTML elements and protect your organization against all others, specify a list of authorized HTML elements.

When a user opens a document that contains a cell with either the Read as HTML or the Read as Hyperlink property in the Web Intelligence HTML viewer or the Interactive Viewer, the viewer may interpret the HTML.

This behavior depends on the way you defined the rendering of these cells in the Web Intelligence display properties and the HTML elements you authorize.

When you specify the authorized HTML elements and a document in Reading mode contains an unauthorized element, only the text from the element is retained – not the element tag or its attributes. In a document that contains an authorized element and both authorized and unauthorized attributes, only the element and authorized attributes are retained.

To authorize only specific HTML elements, in the Web Intelligence display properties for JavaScript, select *Enable only HTML elements defined on the Authorized HTML Elements page* and specify the HTML elements on the *Authorized HTML Elements* page.

By default, only the HTML elements required for Web Intelligence to function correctly are authorized. You can add elements to or remove them from the default list.

> ⚠ Caution
>
> - Web Intelligence enables embedded JavaScript/HTML code in document cells thanks to its formula capabilities.
>   This code can be enabled or disabled in the Central Management Console. However, by authorizing JavaScript, HTMLs and hyperlinks, you acknowledge the risk that you are exposing yourself to Cross-Site Scripting. Cross-Site Scripting allows attackers to alter web sites or execute code on other systems. This vulnerability affects products such as internet browsers when they are running scripts. The majority of Cross-Site Scripting attacks result from insecure programming on the target system.
> - The code can be fine-tuned by a list of authorized HTML tags and attributes. However, SAP is not responsible for the compatibility of this code and its possible side effects. For example, your code might require some adaptation due to browser updates, JavaScript version support or the way the code is dynamically embedded in the web page. From a technical standpoint, as of the 4.3 release, the application runs as a Single Page Application. There is no technical separation between the report and the overall web page. The code might require adjustments to run in that new context
> - Removing elements from the default list impairs Web Intelligence functions so we advise against it.

You can authorize:

- The element `<a>` with the attribute `href` to add a reference.
- A set of attributes for all the elements in your list by associating the element * with the list of attributes. You cannot authorize all the attributes associated with an element.
- Elements that may contain JavaScript, such as `<script>`, `<onClick>`, and `<onMouseEnter>`. You cannot authorize JavaScript keywords.

Example

Authorized HTML elements

Element	Attributes
*	style, class, id
img	src

Element	Attributes
link	ref

The following table shows how Web Intelligence displays HTML elements in documents, as a result of the authorizations.

Impact of the authorizations for HTML elements

Original HTML	Final HTML	Explanation
`<link title="SAP" ref="www.sap.com">`	`<link ref="www.sap.com">`	The `<link>` element and the `ref` attribute are authorized so the link displays as an active link in the document. The `title` attribute is unauthorized so it is removed from the document.
`<img src="datasource" id="I1">`	`<img src="datasource" id="I1">`	The `<img>` element and the associated `src` attribute are authorized and the `id` attribute is authorized for all elements so the original HTML remains.
`<div title="datasource" id="D1">`	Removed.	The `<div>` element is unauthorized so the element and associated attributes are removed from the document.
`<p> ...as shown in the picture below: <img src="../picture.jpg" alt="Mountain"> </p>`	`...as shown in the picture below:<img src="../picture.jpg">`	The `<p>` element is unauthorized so it is removed. Only the text contained in the `<p>` element remains. The `<img>` element and the associated `src` attribute are authorized so they remain. The `alt` attribute is unauthorized so it is removed from the document.

To modify display settings for Web Intelligence [page 643]To modify the list of authorized HTML elements [page 756]

19.4.1 To modify the list of authorized HTML elements

Specify the trustworthy HTML elements that you want to authorize and provide protection against potentially malicious elements by modifying the list of authorized HTML elements.

Prerequisites

Web Intelligence only authorizes the elements that you define on the *Authorized HTML Elements* page when the JavaScript display property *Enable only HTML elements defined on the Authorized HTML Elements page* is active in the Web Intelligence Properties.

Context

Procedure

1. Go to CMC, and select *BI Admin Studio*.
2. From the *Central Management Console Home*, scroll down to *HTML Elements*.
3. Modify the list as described in the following table:

Modification	Steps
To add an element	Click *Add a new element* and enter the element and associated attributes to authorize. **Note** • To authorize certain attributes for all HTML elements, enter * as the element and add the attributes. • When you attempt to add an HTML element that was already on the list, only new attributes for the element are added to the list.
To edit an element	Click the element and click *Edit the selected element.*
To remove an element	Click the element and click *Delete the selected element.*
To restore the default list of authorized HTML elements	Click *Reset.* The default list contains only the elements required for Web Intelligence to work correctly.

20 CMS Reporting

20.1 CMS Reporting

Before you start reporting on the CMS, you need to have a basic understanding of the following concepts:

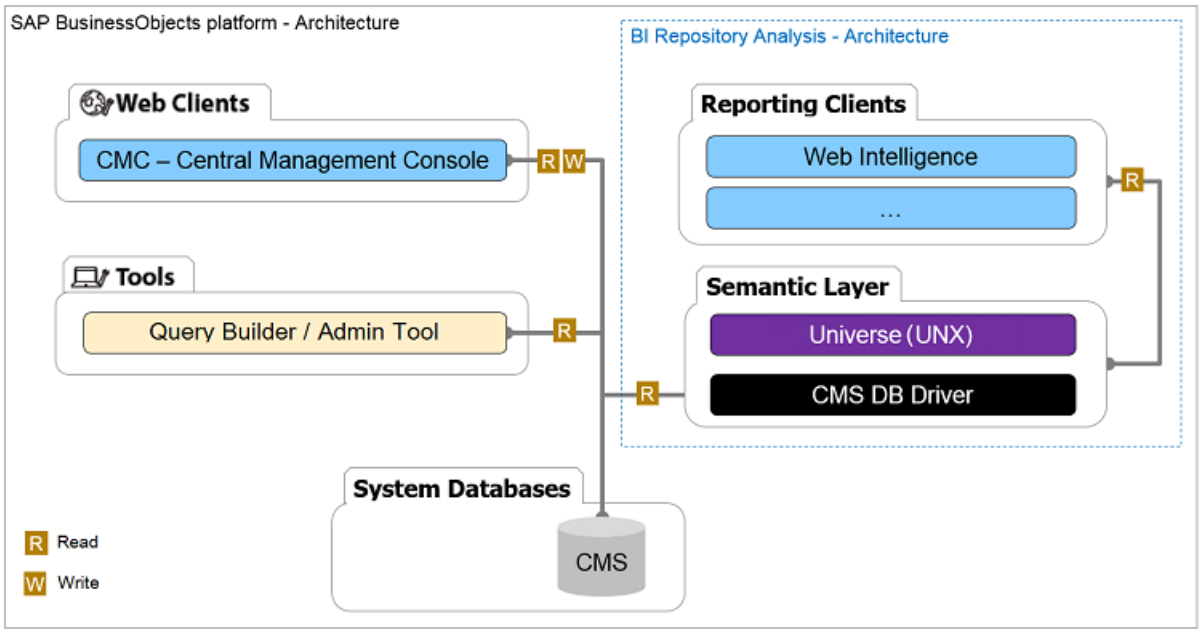
- The architecture of the SAP BusinessObjects platform
- The structure of the CMS system database
- InfoObject properties and relationships

Related Information

The architecture of the SAP BusinessObjects platform [page 757]
The structure of the CMS system database [page 758]

20.1.1 The architecture of the SAP BusinessObjects platform

The schema is designed to help you understand the architecture of the SAP BusinessObjects platform.



The following table provides you more information on the components of the SAP BusinessObjects platform.

The components of the SAP businessObjects platform

Components	Description
CMC - Central Management Console	A web based tool that you use to configure security settings and manage the following items: • User • Content • Server
CMS system database	A database that stores the following BI platform information: • User • Server • Document • Configuration • Authentication The CMS system database is maintained by the Central Management Server (CMS) and can be referred as the system repository.
Query Builder (also referred as Admin Tool)	A web-based tool that you use to query the BusinessObjects repository and get the required information that cannot be found in CMC.
BI Repository Analysis	This solution uses the Semantic Layer of the BI platform, Universe (UNX) and CMS DB Driver to query the CMS.

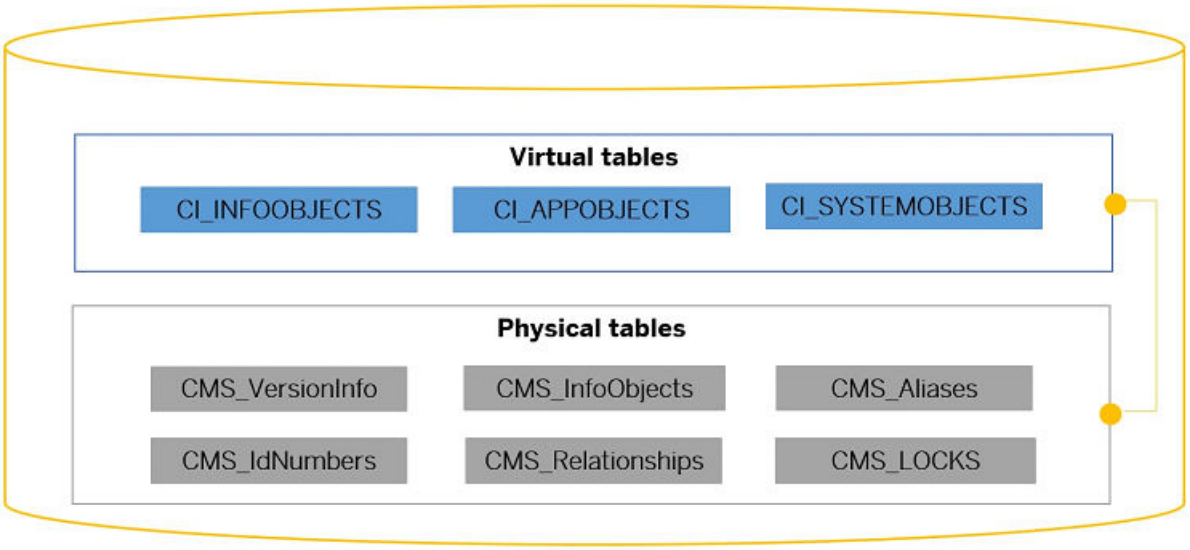
20.1.2 The structure of the CMS system database

The CMS system database is maintained by the Central Management Server (CMS) and can be referred as the system repository. The CMS system is a database which stores BI Platform information in the form of InfoObjects.

The CMS system database includes two kinds of table:

- Physical database table: the CMS metadata is stored in physical database tables.
- Virtual table: the CMS server browses the InfoObjects from virtual tables.

The following schema provides you an overview of the CMS system database structure.



For more information on the CMS system database structure, see the related topics.

Related Information

Physical database tables [page 759]
Virtual tables [page 760]

20.1.2.1 Physical database tables

The CMS metadata is stored in six physical database tables.

Physical database tables

Physical table	Description
CMS_VersionInfo	Includes the current version of BusinessObjects Enterprise (BOE)
CMS_InfoObjects	Main table in the system repository. Each row stores a single InfoObject.
CMS_Aliases	Maps the user alias(es) to the corresponding user ID. A user has an alias for each security domain in which the user is a member. However, a user only has one user ID.
CMS_IdNumbers	Generates unique Object IDs and Type IDs.

Physical table	Description
CMS_Relationships	Stores the relations between InfoObjects.
CMS_LOCKS	Auxiliary table of CMS_RELATIONS

20.1.2.2 Virtual tables

The CMS server browses the InfoObjects from three virtual tables.

Virtual tables

Virtual table	Description
InfoObjects table	Includes InfoObjects that the end user can view, such as: • Report documents • Programs • Shortcuts • Folders • Categories • Inboxes
App Objects table	Includes InfoObjects that documents use, such as: • Universes • Connections • Overloads
System Objects table	Includes InfoObjects that the BI Platform uses to function, such as: • Users • Groups • License keys

20.1.3 About InfoObjects

Before you query the InfoObject metadata, you need to have a clear understanding of the following concepts:

- InfoObject properties
- Relationships between InfoObjects

If you understand how the InfoObjects are organized in the CMS repository, you will be able to quickly and easily browse the repository and fix issues related to the CMS repository.

Related Information

InfoObject properties [page 761]
Relationships between InfoObjects [page 761]

20.1.3.1 InfoObject properties

The following table includes the most important properties for InfoObjects and their descriptions.

InfoObject properties

InfoObject properties	Description
SI_NAME	The name of the object
SI_KIND	The kind of object
SI_OWNER	The user name of the owner
SI_OWNERID	The user ID of the owner
SI_CHILDREN	The number of children
SI_CUID	CUIDs are Cluster Unique Identifiers that uniquely identify an InfoObject
SI_UNIVERSE	The universes (UNX) used by the document

20.1.3.2 Relationships between InfoObjects

The InfoObjects are organized into three hierarchies:

- Folder hierarchy
- User/user group hierarchy
- Server/server group hierarchy

The CMS and client applications use the folder hierarchy to navigate through InfoObjects.

For more information on the relationships between InfoObjects, see the related topics.

Related Information

Folder hierarchy [page 762]
Root folders [page 762]

20.1.3.2.1 Folder hierarchy

The folder hierarchy is a flat list created from an InfoObject's parent. All InfoObjects need to have one parent defined in the property SI_PARENTID.

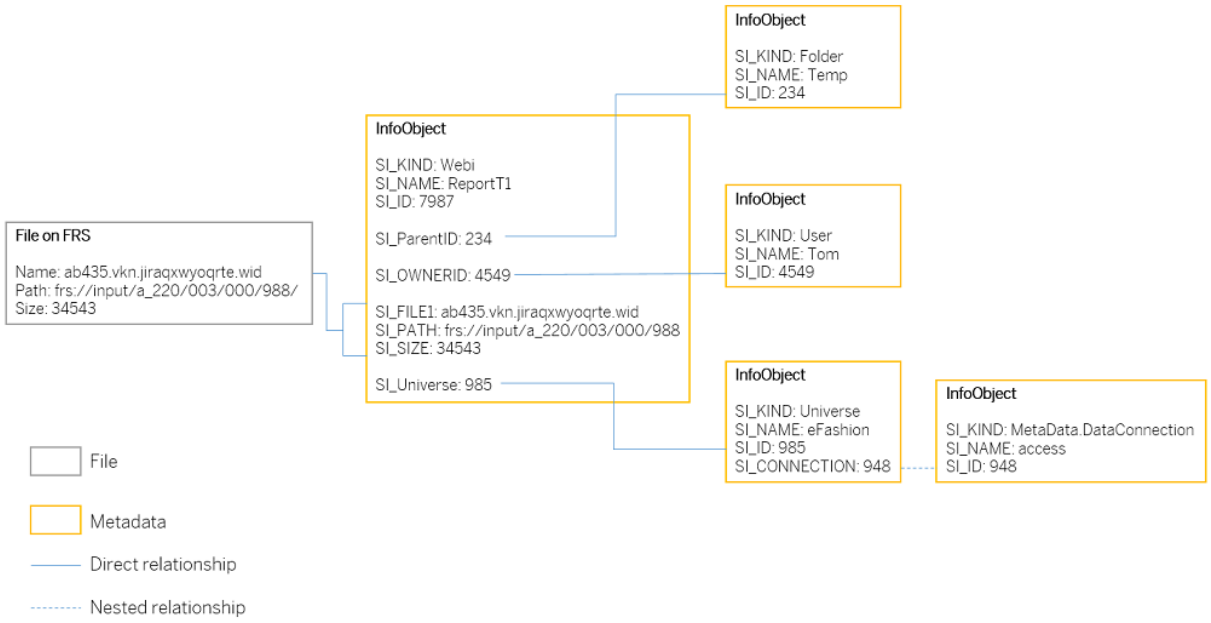
The CMS uses the parent ID property to create the folder hierarchy which is virtual. Indeed, the hierarchy does not correspond to the way InfoObjects are stored in the repository.

20.1.3.2.2 Root folders

The top folder in the CMS Repository hierarchy is the CMS Cluster folders. Root folders can be found at a level below the CMS Cluster folder. Root folders are virtual and do not correspond to anything on the file system.

InfoObjects are organized into root folders for the CMS and client applications to easily and quickly find them. For instance, client applications can navigate through the collection of InfoObjects by first using the InfoObject's root folder, then the parent ID property and children ID properties. The same kind of InfoObjects can usually be found under the same root folder.

The following diagram helps you understand the relationships between InfoObjects.



As you can see, the structure of the InfoObject allows InfoObjects to have an infinite number of relationships and nested relationships.

20.2 Overview of CMS reporting

As an administrator, you need to understand and optimize the usage of the Business Intelligence platform. The CMS reporting sample kit includes the CMS database driver which allows you to visualize and report on

the metadata objects of the CMS database. You can now use a universe and native reporting clients to query the metadata objects of the CMS repository database. These metadata objects include Business Intelligence platform information, such as:

- Connections
- Documents
- Schedules
- Universes
- Users

You can import the CMS reporting sample that contains predefined objects to help you create reports and dashboards using the following SAP BusinessObjects data analysis and reporting applications :

- SAP BusinessObjects Web Intelligence

For a quick and easy way to start reporting on the CMS, you can work with the CMS reporting sample kit. Here are the main stages to create a CMS report:

- Import the CMS reporting sample: You use Promotion Management in the CMC to import the CMS reporting sample.
- Create a CMS report: With SAP BusinessObjects Web Intelligence, you can create a CMS report using the CMS sample universe as a data source.

See Related Information for an end to end procedure that gives a more detailed overview of the creation process.

Related Information

Importing the CMS reporting sample kit with Promotion Management [page 765]

20.3 CMS database connection

You use a CMS database driver to create a secure connection to the CMS database. You can either use the default connection available in the CMS reporting sample or you can create your own CMS database connection.

For the CMS database connection, you need to use a relational connection. The following table describes the parameters of a relational connection.

Parameters for a relational connection

Parameter	Description
Authentication Mode	The method used to authenticate the user's login credentials when accessing the data source: • *Use specified user name, password and System ID*: Uses the *User Name* and *Password* parameters defined for the connection. You can access the data source from either an on premise system or a distant system. **Note** Make sure that the user has the rights to see the content of this session. • *Use Session Token*: Uses the current user session. You can only see the content you are allowed to see and work with. You can only access the data source from an on premise system. **Note** For security matters, this authentication mode is the recommended choice.
System ID	The name of the CMS if *Authentication Mode* is *Use specified user name and password*.
User Name	The user name to access the data source if *Authentication Mode* is *Use specified user name and password*.
Password	The password to access the data source if *Authentication Mode* is *Use specified user name and password*.

20.4 CMS reporting sample kit

You need to use the CMS reporting sample kit to start building documents for CMS reporting. The CMS database driver is integrated in the Business Intelligence platform and the CMS reporting sample can be found in the following location:

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`.

This sample includes the following:

- Connection (BI platform CMS system database.cns)
- Universe (BI platform CMS system database.unx)
- Web Intelligence samples

Find more information about CMS reporting on the SAP Community network.

Related Information

Importing the CMS reporting sample kit with Promotion Management [page 765]

20.4.1 Importing the CMS reporting sample kit with Promotion Management

Prerequisites

Before you begin, make sure that you have access to the CMS reporting sample which is in the following location:

```
<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI
on BI
```

Context

You use the Promotion Management tool in the Central Management Console (CMC) to import the CMS reporting sample.

Procedure

1. In the Central Management Console, click *Promotion Management*.
2. Click *Import* > *Import File*.
3. Select *File System*
4. Click *Choose file* to select the sample.
5. In the *New Job* pane, select *Login to a New CMS* for the *Destination* field.
6. Enter the login parameters then click *Login* > *Create*.
7. In the *Promotion Jobs* pane, right-click the sample then select *Promote*.
8. In the *Promote* dialog box, click *Promote*.

Results

When the *Promotion Status* of the CMS reporting sample is *Success*, you have successfully imported the sample into your Business Intelligence 4.2 system. To use the sample universe for CMS reporting, see the related topic.

Related Information

CMS reporting sample kit [page 764]

20.4.2 The CMS sample universe

The CMS sample universe includes a predefined universe that supports common reporting scenarios. According to your analysis and reporting needs, you can edit and enhance the predefined universe. You can also find a list of predefined queries in the *Queries* pane. These queries can serve as a tutorial for the universe features.

Some of the most useful queries and what they mean are listed in the table.

Useful queries to run on the CMS universe

Query	Description
Sample-User-Relationship-Detail	Allows you to see in which group a user belongs to.
Sample-FolderPath (Universe)	Allows you to find the location of an universe.
Sample-ScheduleInfo-Relationships	Allows you to visualize the actions scheduled by the users.
Sample-QT-Properties with Filter (Server)	Allows you to visualize the properties of an InfoObject.

20.4.3 Extending the CMS sample universe

You can create a linked universe to expand the CMS sample universe. A linked universe is a .UNX universe that contains a link to a designated core universe in the CMS.

In this case, the CMS sample universe acts as a core universe so the linked universe can use the CMS sample universe's data foundation and business layer as pre-fabricated building blocks. Once you have created the linked universe, you can save its data foundation and business layer inherited from the CMS sample universe as new files so they have a life cycle independent of the CMS sample universe.

You can use the CMS database connection of the CMS sample universe or another connection compatible with the CMS database.

You can add tables, create joins linking the core data foundation tables with the new ones, and add new components to the business layer in the same way that you do for any other universe. Any changes in the core components are automatically propagated to the linked universe when it is checked into the CMS.

20.5 Creating a report on CMS

With SAP BusinessObjects Web Intelligence, you can create a report on CMS using the CMS sample universe as a data source.

Procedure

1. Open Web Intelligence and click the *New* icon in the *File* toolbar.
2. Select the CMS sample universe.

   If you are using the Web Intelligence Rich Client, click *Select*.

   The *Query Panel* opens.
3. Select and drag dimensions and measures that you want to include in the query into the *Result Objects* pane.
4. Select the objects on which you want to define query filters and drag them to the *Query Filters* pane. To create a quick filter on an object, select the object in the *Result Objects* pane then click the *Add a quick filter* icon in the *Result Objects* toolbar.
5. Click *Run Query*.

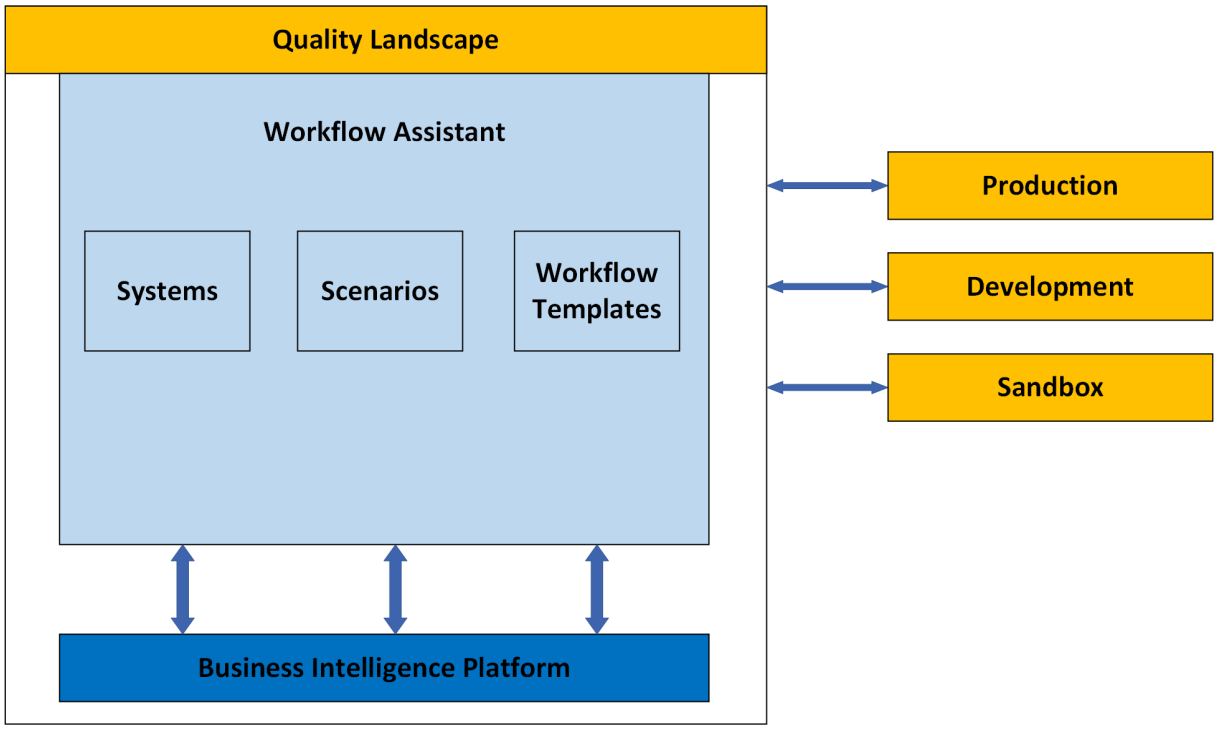
21 Workflow Assistant

Automation Framework and Agent services are now merged into one service called as Workflow Assistant service. Workflow Assistant is an application in the Central Management Console (CMC) for administration of BI systems and automation of BI tasks.

> **Note**
>
> Automation Framework functionality in BI Admin console is now achieved through Workflow Assistant. The BI Admin Console URL (`http://<systemName>:<portNo>/BOE/BIAdminConsole`) and the message queue service is now deprecated.

Workflow Assistant displays the content as tabs: *Scenarios*, *Workflow Templates*, and *Systems*. From these tabs, you can drill down into the relevant section for more detailed information and functions.

Workflow Assistant implements a role-based concept so that users only have access to those tabs for which they are authorized.



About Systems

System refers to one or more BI machines that you are authorized to access. System management is an application that lets you access and manage your BI landscapes centrally. To avail the capabilities of Workflow Assistant, it is essential to first register your BI landscapes using the System Management application.

About the Workflow Assistant

Workflow Assistant provides you the capability to simplify complex and repetitive BI tasks.

> **Example**
>
> Consider that you have to perform the following BI tasks in order:
>
> 1. Logon to the BI platform.
> 2. Change the source of certain Web Intelligence documents from `.unv` to `.unx`.
> 3. Refresh these Web Intelligence documents.
> 4. Log out of the BI platform.

The manual effort is reduced with Workflow Assistant. You can create a scenario using task and workflow templates, save this scenario, execute (run), and view the results.

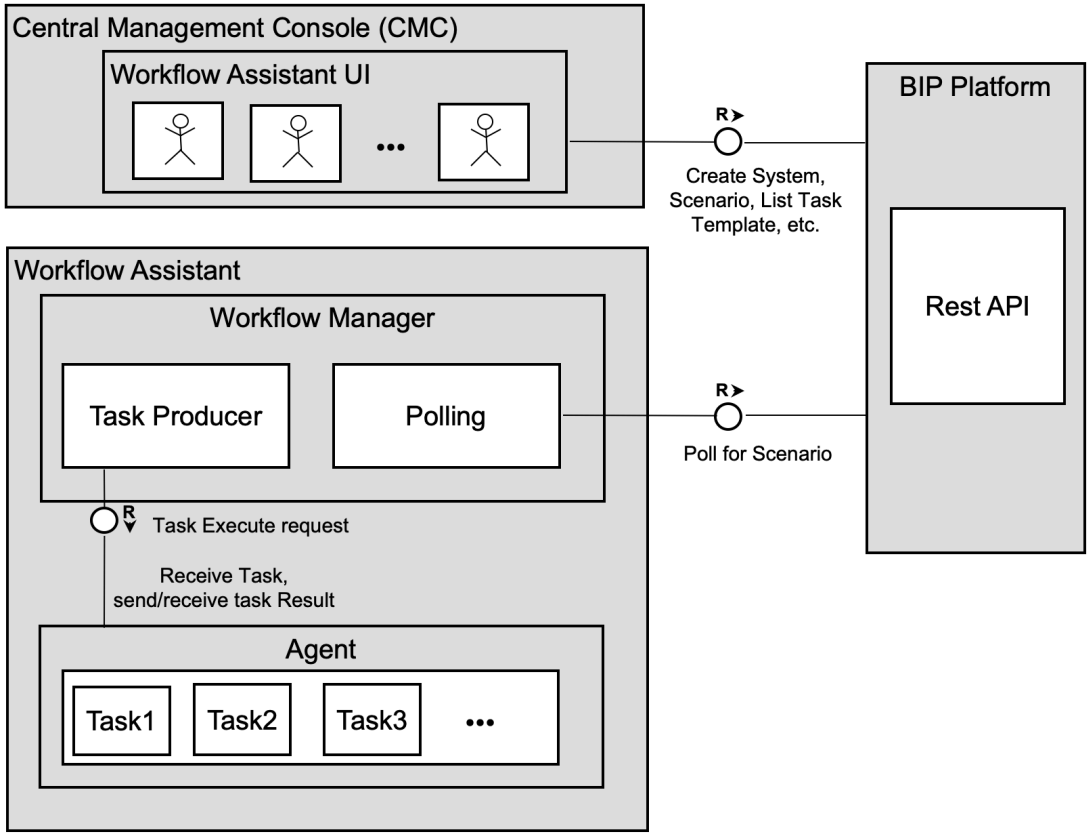
21.1 Target Audience

This guide is intended for certain users of the Business Intelligence (BI) platform and certain BI platform developers.

- BI platform users who use this guide should have rights to access the Central Management Console (CMC) and the Workflow Assistant. These users have the role of administrators or delegated administrators.
- BI platform developers who use this guide should be conversant with working on Java SDKs who can create JSON schemas for custom requirements by using the Task Template SDK.

21.2 Understanding the Architecture

The below diagram helps you understand the Workflow Assistant architecture and the inter-connections between its components.



Glossary of Terms Used in the Above Diagram:

Term	Definition
Workflow assistant UI	A UI to create workflow templates and scenarios that can be executed on any given system.
Workflow manager	A workflow manager polls scenarios from platform, manages the execution of the scenarios, and saves the results.
Agent	It's a lightweight process to execute the tasks within scenarios.

21.3 Glossary

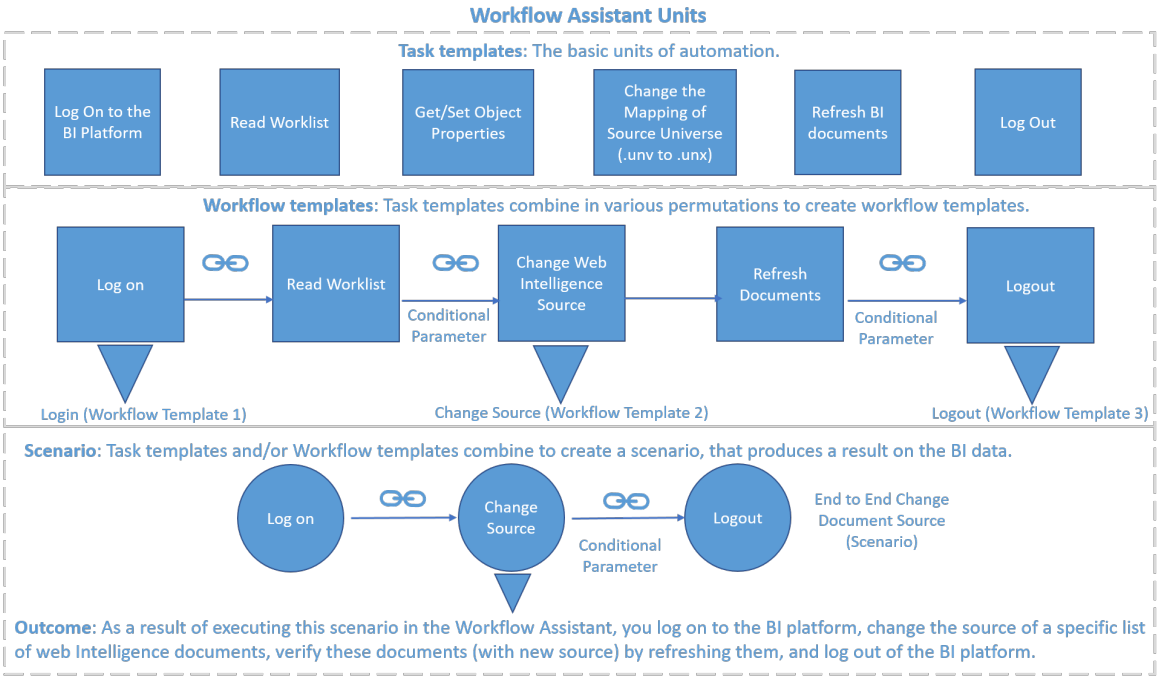
The Workflow Assistant has its own specialized vocabulary.

Frequently Used Terms in the Workflow Assistant

Term	Definition
Standard Task Template	The basic unit of automation provided by default in the application. These units can be used in scenarios or workflow templates. For example, a simple task such as logging on to the BI platform, refreshing BI documents, reading data, changing the mapping of source Universe of Web Intelligence documents (from unv to unx), adding users to your landscape or logging out.
Custom Task Template	A task template (basic unit of automation) which is created by developers for custom requirements. **⚠ Restriction** You cannot create a custom task template using the UI of Workflow Assistant. It requires the Task Template SDK.
Workflow Template	A logical group of task templates ordered in the required sequence to achieve the outcome of a workflow.
Standard Workflow Template	Workflow templates which are provided out of-the-box in the Workflow Assistant. Administrators can readily use standard workflow templates when creating scenarios for their various BI automation requirements.
Custom Workflow Template	A workflow template created by administrators for their custom requirements. It is created in the Workflow Assistant by grouping standard or custom task templates.
Scenario	An executable entity which is created using task templates or workflow templates in the required sequence.

Term	Definition
Conditional Parameter	The connecting link between task templates or workflow templates, which directs the flow of control, is based on one of the following conditions: • Continue (default) • On success • On failure • On partial success **Note** A conditional parameter also lets you insert a *"Time Delay"*(in seconds) to ensure that the next task in the scenario starts only after a certain time duration once the previous task execution is completed. **→ Remember** The Workflow Assistant considers the conditional parameter value: 'Continue', only if the previous task has completed with either of the three states : 'Success', 'Partial Success' or 'Failure'. If the previous task has the status of 'Error' or 'Not Executed', the state of next node is automatically set to 'Not-executed'.

This illustration will help you understand the interconnection between some of the above terms:



21.4 About Installation and Update

Depending on whether you make a fresh installation or update an existing installation, your access to back-end functionality may be different.

When you make a **fresh installation** of SAP BusinessObjects BI platform (default installation), you gain full access to the Workflow Assistant on the machines where you have installed and configured the BI platform. This includes access to the Workflow Assistant application in the CMC and the back-end functionality (Workflow Assistant Service).

However, now when you update from the BI platform SP5 or later to 4.3, the complete functionality of Workflow Assistant is available, but you will still need to run through the SAP Note mentioned under Restrictions. After installing the update, run the "Modify" installation workflow to get the backend services. For more information on Modify installation, refer to the *Support Package Update Guide* posted on SAP Business Intelligence platform page of Help portal .

> **Note**
>
> Workflow Assistant is a part of the BOE.war file. After you update from the BI platform 4.2 SP4 or earlier to 4.2 SP5 and above version, the web application is deployed only if the *Java Web Applications* functionality was selected during the installation of the existing version.

> **Caution**
>
> You should not install the Workflow Assistant in multiple machines within systems as clustering of Workflow Assistant is not supported.

> ⚠ Restriction
>
> When you update from the BI platform 4.2 SP4 or earlier to 4.2 SP5 or later, you observe that some of the folders are not listed in Workflow Assistant. For more information, refer to 2882649.

21.5 Configuring the Workflow Assistant

When you install the Workflow Assistant as part of the BI platform installation, you obtain the service by default in your set up.

You can then configure trusted authentication to start using the Workflow Assistant.

21.5.1 Basic Configuration

21.5.1.1 Configuring Enterprise Authentication for Workflow Assistant

Prerequisites

You have installed the Workflow Assistant as part of the BI platform installation in your set-up.

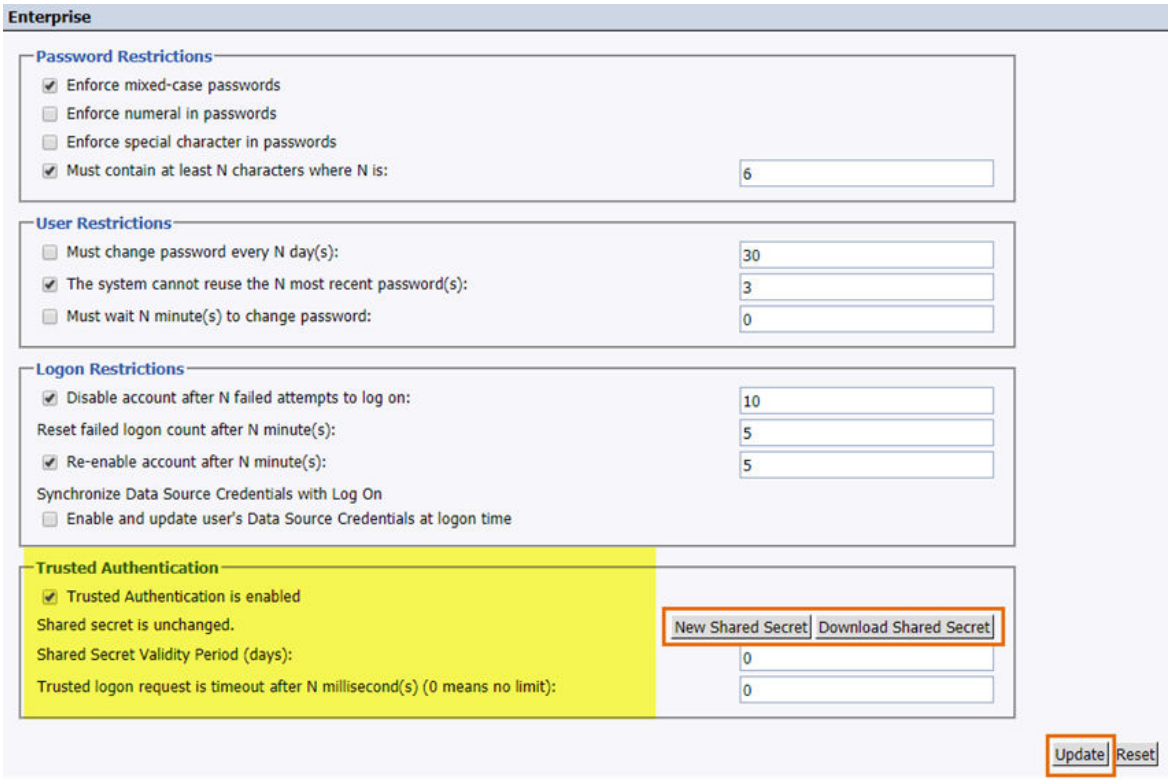
Context

To configure trusted (Enterprise) authentication for the Workflow Assistant, follow the procedure given below:

Procedure

1. Log on to the Central Management Console (CMC) by connecting to the CMS of the master node.
2. Select *Authentication* in the drop-down, then double-click on *Enterprise*.

The 'Enterprise' dialogue appears as shown below:



3. In the 'Trusted Authentication' section, ensure that *Trusted Authentication* is enabled.
4. Choose *New Shared Secret*.
   The Shared secret key is generated.
5. Choose *Download Shared Secret*.
6. Select *Update*.
7. Save the generated Shared Secret Key (TrustedPrincipal.conf):
   a. In Windows, at `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0\win64_x64/`.
   b. In Linux, at `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`.

> **Note**
>
> For more information on how to create trusted authentication certificates with different options, refer to the topic Enabling Trusted Authentication [page 243].

21.5.1.2 Creating a Default User for Workflow Assistant Backend Service

Procedure

1. Create a new user in the Workflow Assistant with the name **WAUser**.
2. Assign appropriate rights by going to `Workflow Assistant` folder, and granting Full Control to the **WAUser** account.

   The Workflow Assistant backend service starts using the **WAUser** account.

   If the **WAUser** acount doesn't exist, Workflow Assistant starts using the *Administrator* account.

   > ⓘ Note
   >
   > It is not mandatory for the new user to be a part of the *Administrator* user group.

21.5.1.3 Starting Workflow Assistant Service

The topic provides instructions to start *Workflow Assistant Service*.

Procedure

1. Configure enterprise authentication for Workflow Assistant. Refer to Configuring Enterprise Authentication for Workflow Assistant [page 774] for more information.
2. To start the *Workflow Assistant Service*:
   a. In Windows, launch *Central Configuration Manager* (CCM), and start *Workflow Assistant Service*.
   b. In Unix, go to `<INSTALLDIR>/AdminConsole/WorkflowAssistant/startWfAssistant.sh`.

   You are now ready to use the *Workflow Assistant* and execute scenarios.

   > ⓘ Note
   >
   > To ensure that Workflow Assistant is succesfully started, check the content of the `message.properties` file in `<BOE-Install-Directory>\AdminConsole\WorkflowAssistant\service-logs`. The `message.properties` content should be:
   >
   > ```
   > STATUS_WFM=success
   > MESSAGE_AGENT=Agent - Started\!\!
   > STATUS_AGENT=success
   > ```

```
MESSAGE_WFM=Workflow Assistant - Started\!\!
```

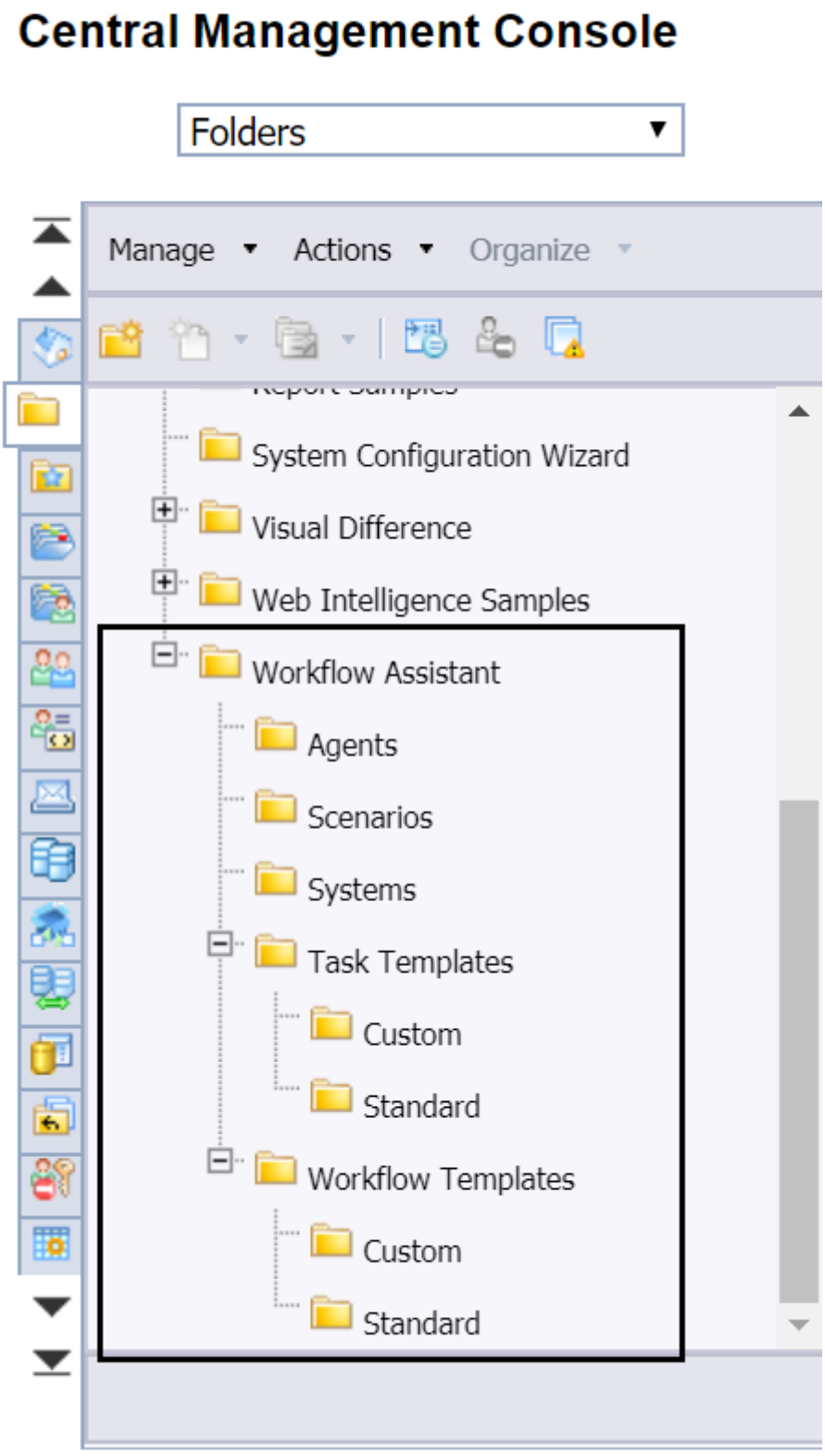
21.6 Managing Workflow Assistant Rights Via the Central Management Console

You manage security for the Workflow Assistant via the Central Management Console.

Workflow Assistant is listed under *Applications* of the *Central Management Console*.

You can view and manage the access rights and overall security settings for the following entities in Workflow Assistant:

- Systems
- Scenarios
- Task Templates
- Workflow Templates



For information on how to manage security settings for objects in the CMC, refer to the topic Managing security settings for objects in the CMC.

> **Note**
>
> - You can control the access to a functionality in Workflow Assistant such as *Systems*, *Scenarios*, *Task Templates*, and *Workflow Templates* by assigning rights at the folder or object level to the user, but the lack of rights has no impact on the user interface. This means a user should have the right *Add Objects to this folder* on the *Scenario* folder to create a scenario.
> - For example, the user can see an option to create a scenario in Workflow Assistant even if the user has no rights on the *Scenario* folder in CMC. If the user still tries to create and save a scenario in the *Scenario* folder, then the system would prompt an error message.

Managing Application Rights

With appropriate application specific rights, you can decline or carry out the following tasks in Workflow Assistant:

- To decline a *Create Task Template*, go to Task Template folder and decline *Add objects to the folder*.
- To decline a *Create Workflow Template*, go to Workflow Template folder and decline *Add objects to the folder*.
- To decline a *Create Scenario*, go to Scenario folder and decline *Add objects to the folder*.
- To decline a *Edit Task Template*, go to Task Template folder and decline *Edit objects*.
- To decline a *Edit Task Template that the user owns*, go to Task Template folder and decline *Edit objects that the user owns*.
- To decline a *Edit Workflow Template*, go to Workflow Template folder and decline *Edit objects*.
- To decline a *Edit Workflow Template that the user owns*, go to Workflow Template folder and decline *Edit objects that the user owns*.
- To decline a *Edit Scenario*, go to Scenario folder and decline *Edit objects*.
- To decline a *Edit Scenario that the user owns*, go to Scenario folder and decline *Edit objects that the user owns*.
- To decline a *View Task Template*, go to Task Template folder and decline *View objects*.
- To decline a *View Task Template that the user owns*, go to Task Template folder and decline *View objects that the user owns*.
- To decline a *View Workflow Template*, go to Workflow Template folder and decline *View objects*.
- To decline a *View Workflow Template that the user owns*, go to Workflow Template folder and decline *View objects that the user owns*.
- To decline a *View Scenario*, go to Scenario folder and decline *View objects*.
- To decline a *View Scenario that the user owns*, go to Scenario folder and decline *View objects that the user owns*.
- To decline a *Delete Task Template*, go to Task Template folder and decline *Delete objects*.
- To decline a *Delete Task Template that the user owns*, go to Task Template folder and decline *Delete objects that the user owns*.
- To decline a *Delete Workflow Template*, go to Workflow Template folder and decline *Delete objects*.
- To decline a *Delete Workflow Template that the user owns*, go to Workflow Template folder and decline *Delete objects that the user owns*.
- To decline a *Delete Scenario*, go to Scenario folder and decline *Delete objects*.

- To decline a *Delete Scenario that the user owns*, go to Scenario folder and decline *Delete objects that the user owns*.
- To decline a *Run Scenario for all combinations*, go to given scenario and decline *Add objects to the folder*.
- To decline a *Run Scenario that the user owns for all combinations*, go to given scenario and decline *Add objects to folder that the user owns*.
- To decline a *Create Landscape*, go to Landscape folder and decline *Add objects to the folder*.
- To decline a *Edit and View Landscape*, go to Landscape folder and decline *Edit objects* and *View objects*.
- To decline a *Delete Landscape*, go to Landscape folder and decline *Delete objects*.
- To decline a *Add user credentials on landscape*, go to Landscape folder and decline *Add objects to the folder*.

> **Note**
>
> All the above mentioned rights can be applied to individual Task template/Workflow template/Scenario.

21.7 Working with the Workflow Assistant

The Workflow Assistant is an application in the CMC that lets you automate your repetitive and complex BI Administration tasks. In the following sections, you are going to learn how you can automate the BI Administration tasks.

21.7.1 About Standard Task Templates

Standard task templates are provided in-built (out-of-the-box) with the Workflow Assistant. When creating scenarios or workflow templates, you can use these task templates.

Standard Task Template	Description
Logon	Establishes a session with the target BI platform server.
Refresh Documents	Opens and refreshes the list of provided documents using the `<Schedule now>` operation. **Note** For documents with prompts, the default values must be specified in the documents before execution.
Change Web Intelligence Source	Changes the mapping of source universe for your list of documents from .unv to .unx, .unx to .unx, or .unv to .bex.
Add/Remove User & User Group	Adds or removes users and user groups to the BI landscape.

Standard Task Template	Description
	Note This task template corresponds to the `<Import functionality>` on the BI platform. For information on the Import functionality, refer to the topic To add users or user groups in bulk.
Get Properties	Returns the values of certain properties for the queried InfoObjects.
Set Properties	Sets the values of certain properties for the given InfoObjects in the CMS.
Read Worklist	Reads .CSV files as an input and returns the comma separated values which can be consumed by subsequent tasks. Use this task template when a large number of values (bulk data) must be consumed by workflow templates in your scenario and it is not feasible to manually feed the values using the Input panel of Workflow Assistant.
Query Worklist	Queries the CMS tables and provides the output in CSV format.
Save Output	Saves the values obtained from the *Output Parameter* of a task into a CSV file in the CMS.
Set Server Properties	Sets the values of certain properties for the given Server(s)
Logout	Ends the task session with the target BI platform server.

21.7.1.1 Log On

Parameters for Log On Task Template

Input Parameters

Name	Type	Description
System	String	Name of the registered landscape in the Workflow Assistant

21.7.1.2 Refresh Documents

Parameters for Refresh Documents

Input Parameter

Name	Type	Description
*Documents	CSV	Document identifiers (id/cuid) for documents that need to be refreshed. A user can also choose documents from Repository Explorer through Value Help. CSV format: id or cuid

Output Parameters

Name	Type	Description
SuccessfullyRefreshedDocuments	CSV	Documents that are successfully refreshed. CSV format: id, cuid
UnsuccessfullyRefreshedDocuments	CSV	Documents that are not successfully refreshed. CSV format: id, cuid
All	CSV	List of processed documents. CSV format: id, cuid

21.7.1.3 Change Web Intelligence Source

Parameters for Change Web Intelligence Source

Input Parameters

Type	Description
CSV	Specify the Web Intelligence document's cuid for which you wish to replace the UNV with UNX, UNX with UNX, or UNV with BEx. A user can also choose documents from Repository Explorer through Value Help or by mapping an output of one task to another. CSV format: id or cuid
CSV	Mapping Universes (UNV, UNX, BEx) based on id or cuid. A user can also map the universes through the Universe Mapping screen in Value Help. CSV format (for UNV-UNX): unv_cuid, unx_cuid or unv_id, unx_id CSV format (for UNX-UNX): src_cuid,dest_cuid,type CSV format (for UNV-BEx): src_cuid,dest_cuid,type,technical_name
String	To change source without saving the document, assign the value: 'Test' To change source and save the document, assign the value: 'Change'

Output Parameters

Name	Type	Description
Success	CSV	Documents for which the source is successfully changed. CSV format: id, cuid
Failure	CSV	Documents for which the source failed to change. CSV format: id, cuid
All	CSV	List of input documents. CSV format: id, cuid

21.7.1.4 Add/Remove User and User Group

Parameters for Add/Remove User and User Group

Input Parameters

Name	Type	Description

*Data	CSV	User specific information.
		See the sample CSV data below. For more information on CSV data, see the topic *To add users or user group in bulk* in the *Business Intelligence Platform Administrator Guide*.
		`command,group,user,fullname,password,mail,profileName,profileValue`
		`Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue`

> **Note**
>
> You can also create a CSV file without a CSV header and use it as an input to your scenario.
>
> The password chosen in the CSV file must adhere to password policy.

> **Tip**
>
> You can use consecutive commas to skip an input field.

21.7.1.5 Get Properties

Parameters for Get Properties

Input Parameters

Name	Type	Description
*InfoObject	CSV	CSV values for InfoObjects. The prefix 'si_' should not be specified for using the properties. CSV format: id or cuid
*Property	CSV	CSV values of properties. The prefix 'si_' should not be specified for using the properties. For a user's InfoObjects, the supported property is 'property;data'.

Output Parameters

Name	Type	Description
Success	CSV	List of InfoObjects for which the property value was successfully searched or assigned. CSV format: id or <searched property>
Failure	CSV	List of InfoObjects for which the property value could not be successfully searched or assigned. CSV format: id, cuid
All	CSV	List of all processed InfoObjects. CSV format: id, cuid

21.7.1.6 Set Properties

Parameters for Set Properties

Input Parameters

Name	Type	Description
*InfoObject	CSV	CSV values for InfoObjects. The prefix 'si_' should not be specified for using the properties. CSV format: id or cuid
*Property	CSV	CSV values of properties. For a user's InfoObjects, the supported property is 'property;data'.

Output Parameters

Name	Type	Description
Success	CSV	List of InfoObjects for which the property value was successfully fetched or set. CSV format: id or <searched property>
Failure	CSV	List of InfoObjects for which the property value could not be successfully fetched or set. CSV format: id, cuid
All	CSV	List of all processed InfoObjects. CSV format: id, cuid

21.7.1.7 Set Server Properties

Parameters for Set Server Properties

Input Parameters

Name	Type	Description
*Server	CSV	Identifiers (id/cuid) for servers that need to be changed. A user can also choose servers from Repository Explorer through Value Help. CSV format: id or cuid
*Property	CSV	CSV values with property and value. For example: `hostname;new value`. Supported properties: hostname

Output Parameters

Name	Type	Description
Success	CSV	List of Servers for which the property value was successfully set. CSV format: id
Failure	CSV	List of Servers for which the property value could not be successfully set. CSV format: id
All	CSV	List of all processed Servers. CSV format: id

21.7.1.8 Read Worklist

Parameters for Read Worklist

Input Parameters

Name	Type	Description
*File	CSV	CSV file with the required data for reading. A user can also choose a CSV file from Repository Explorer through Value Help. CSV format: <Header1>, <Header2>, ..<HeaderN> **Note** To know more about the Data Formats and Delimiters in CSV, refer to Working with CSV Data [page 797].

Output Parameters

Name	Type	Description
Values	CSV	The list of values read from the input file which are returned in comma separated format.

21.7.1.9 Save Output

Parameters for Save Output Task

Input Parameters

Name	Type	Description
*Parameter	CSV	Map the output obtained from the previous task.

Name	Type	Description
*File name	String	Specify the file name to save the output.
*Choose destination folder	String	Select the folder to which the file must be saved.
*Save options	String	To overwrite a file that exists with the same name, choose the value: *Overwrite*. To rename a file that exists with the same name with suffix _1, _2,..., choose the value: *Rename*.

> ⓘ Note
>
> **Output Parameter:**
>
> Output obtained is a file in CMS. Hence, no parameter is available for consumption.

21.7.1.10 Logout

Parameters for Logout Task

Input Parameter

Name	Type	Description
SessionToken	String	Session token (generated because of the logon)

21.7.2 About Standard Workflow Templates

Standard workflow templates are provided in-built (out-of-the-box) with the Workflow Assistant. When creating scenarios, you can use these workflow templates.

Standard Workflow Templates Available in the Workflow Assistant

Template Name	Description
Logon	Establishes a session with the target BI platform server.

Template Name	Description
Refresh Documents	Refreshes the specified list of Web Intelligence documents.
Change Document Ownership	Queries for owner of the document and assigns the same owner to a different document.
Change User License Type	Queries for users list based on user-specific conditions and changes the license type.
Change Web Intelligence Source & Verify the Documents	Changes the mapping of source universe from .unv to .unx, .unx to .unx, or .unv to .bex and validates the documents for Web Intelligence documents in bulk.
Add/Remove Users	Allows an administrator to add or remove users and groups.
Logout	Ends the task session with the target BI platform server.

21.7.3 About Custom Task Templates

You can use the standard task templates in the Workflow Assistant to design workflow templates and execute scenarios. If the standard templates are not enough to fulfill your needs, you can develop your own task template and plugin for Workflow Assistant.

Create your own custom task template using the custom task template SDK that provides an API for the developers to implement new task templates. For more information, refer to https://community.sap.com/t5/technology-blogs-by-sap/how-to-create-a-custom-task-template-for-bi-automation-framework/ba-p/13333292 .

21.7.4 Managing Workflow Templates

You can create, edit, and delete custom workflow templates from the Workflow Assistant.

21.7.4.1 Creating Custom Workflow Templates

You create custom workflow templates by using standard or custom task templates.

Procedure

1. On the Home page, choose *Workflow Assistant*.
2. On the *Workflow Assistant* page, choose the *Workflow Templates* tab.
3. Choose the + (*Add*) icon on the top right of the *Workflow Templates*.
4. In the *Create Workflow Template* canvas, choose the > (*Expand*) icon appearing before the *Standard* and *Custom* categories of task templates in the left panel.
5. Drag and drop the required task templates to the canvas on the right side of the page.
6. Rename your dropped task template within the canvas.
7. (Optional) Choose the (*Link*) icon that appears between two task templates and select the required value for conditional parameters in the list which appears.

   Here, you can also insert the required `<Time Delay>` (in seconds).
8. (Optional) Set values for input parameters, they will be used as default values when the Workflow Template is used in a scenario.
9. Choose *Save*.
10. In the *Save Workflow Template* dialog, enter a name (mandatory) for your workflow template, and add a description if required.
11. Choose *Save* in the *Save Workflow Template* dialog.

    The new workflow template starts listing in the *Workflow Templates* view of the Workflow Assistant.

> ⓘ Note
>
> Any modifications to the existing workflow templates has no impact on the existing scenarios.

21.7.4.2 Editing Custom Workflow Templates

You edit custom workflow templates in the Workflow Assistant.

Procedure

1. In the *Workflow Templates* tab of the Workflow Assistant, choose (*More*) and select *Edit*.
2. In the *Edit Workflow Template* screen, make the required edits to the workflow template by adding/removing the task templates, modifying the input parameter values, or by modifying the conditional parameters between task templates.
3. Choose *Save As*.
4. In the *Save Workflow Template* dialog, modify the name of the workflow template as required.
5. Select *Save*.

   The modifications to the workflow template are saved and you return to the Home page of the Workflow Assistant.

21.7.4.3 Deleting Custom Workflow Templates

You delete custom workflow templates in the Workflow Assistant.

Procedure

1. In the *Workflow Templates* tab of the Workflow Assistant, choose (*More*) and select *Delete*.
2. Choose *Delete* in the warning that appears.

   The deleted workflow template is no longer listed in the *Workflow Templates* tab of the Workflow Assistant.

21.7.5 Managing Scenarios and Viewing Results

Scenarios are created by connecting task templates and workflow templates. You manage scenarios and view results in the Workflow Assistant.

21.7.5.1 Creating Scenarios

This topic explains how you can create scenarios in the Workflow Assistant.

Procedure

1. On the Home page of the CMC, choose *Workflow Assistant*.

   The available scenarios are listed on the page which appears.
2. Click the + (*Create folder or scenario*) icon and select *Scenario*.
3. In the *Create Scenario* page, choose the > (*Expand*) icon appearing before the *Standard* and *Custom* categories of task templates in the left panel.

   > **Note**
   >
   > You can check the task's description by hovering your mouse over the task template's name.
4. Drag and drop the required workflow templates to the canvas on the right side of the page.
5. (Optional) Choose the (*Link*) icon that appears between two task templates and select the required value for conditional parameters in the list which appears.

   Here, you can also insert the required `<Time Delay>` (in seconds).
6. Click on a workflow template in the canvas.

   An input panel appears on the right side of the canvas.
7. In the input panel on the right, choose > (*Expand*) to view the input parameter fields for each task template and make the required value selections in the fields.

   > **Caution**
   >
   > - Ensure that any of the input values that you specify for template parameters does not include your personal data and adheres to the General Data Protection Regulation (GDPR) guidelines. For more information on GDPR, refer to the topic Data Protection and Privacy [page 169].

   > **Note**
   >
   > You can get more information about the parameters by referring to the Parameter Info. For more information on Parameter Info, refer to About Parameter Info [page 798].
8. Choose *Save*.

> → Remember
>
> It is mandatory to specify inputs for each task template in a scenario before you can run a scenario. But, you can also use *Run with Parameter* option to specify the inputs.

9. In the *Save Scenario* dialog box, provide necessary information in the *Save Scenario* and *Notify by E-mail* tabs.
   a. In the *Save Scenario* tab, enter a name (mandatory) for your scenario, add a description, and select a location, where the scenario will be saved.
   b. In the *Notify by E-mail* tab, select the toggle button to switch on.
   The options, as shown in the image below, are

   displayed.
   c. Select one or more options. Your selection is the criteria to trigger an email notification.
   d. You can either *Use Default Setting* or switch it off using the toggle button. These default settings are defined in CMC. See *Business Intelligence Administrator Guide* to learn how to define default settings for email destinations.
   e. If you deselect *Use Default Setting* then, enter *From, To*, *CC* (optional), and *BCC* (optional) e-mail address, *Subject*, and *Message*. You can also add the placeholders to each field.
10. Choose *Save* or *Save & Run*.

    The new scenario is listed in the *Scenarios* view of the *Workflow Assistant* and based on the criteria selected in *Notify by E-mail* tab, the email will be triggered.

21.7.5.1.1 Providing Input Parameters

While creating workflow templates in *Workflow Assistant*, you can add input values during design time and run time. This means that you can add the input values while creating and executing a scenario. There are two ways to add input values to a *Scenario*:

1. Value Help
2. Mapping output of a task as an input of another task

Value Help

You can choose an object like document and worklist from the repository explorer with the *Value Help*. For example, in a scenario to refresh the document, you can choose a document by selecting the *Value Help* icon in the *Documents* field.

Mapping output of a task as an input of another task

You can provide the output of the first task as the input for the second task while executing a scenario. You have to type @ in an input field to see the list of values obtained from the first task.

- The format of an input value is **@<WorkflowTemplate>.<TaskTemplate>.<OutputParameter>**.
- The list of input values shows only the compatible values obtained from the first task. If the input field accepts CSV as the data type for example, the input values from the previous task that are in CSV format are displayed.

> **Note**
>
> The input parameters support CSV file as an input. For more information, refer to Working with CSV Data [page 797].

21.7.5.1.2 Working with CSV Data

Most of the standard task templates support input parameter values in CSV format. For example, the *Document Refresh* task template supports CSV format for the input field *Documents*. This means that you can select a CSV file comprising of data in the format **name, cuid, and status** as an input for *Documents*.

> **Note**
>
> If the task input field accepts **cuid**, and you select a CSV file that contains other parameters including **cuid**, the input field then consumes only the **cuid** column values from the CSV file. For an example, refer to the CSV data below:
>
> name, cuid, status;
>
> Charting, AW4AVT1AUhVAogA6P7OQv9c, success;
>
> SalesReport, BW3AVT1AUhVAogA743QCDsD, success;
>
> In this example, the input field consumes AW4AVT1AUhVAogA6P7OQv9c and BW3AVT1AUhVAogA743QCDsD, and ignores the other values.

Column and Row Delimiter

The supported column delimiter is **,**. The row delimiter is **;**. A column and a row delimiter in an input field separates the data in column and row format. For an example, refer to the CSV data below:

name, cuid, status;

Charting, AW4AVT1AUhVAogA6P7OQv9c, success;

SalesReport, BW3AVT1AUhVAogA743QCDsD, success;

Here, the comma signifies that **name, cuid, and status** are columns, while semi-colon signifies the end of the row.

> **Note**
>
> If a CSV file is an input for *Read Worklist* task template, the column delimiter is then ,. The row delimiter is ; or a new line.

> **Caution**
>
> A value in the CSV data should not contain a comma or a semi-colon.

21.7.5.1.3 About Parameter Info

You can see the Parameter Info after you expand and select any parameter in the input panel of a scenario. For example, in the task template Refresh Documents, there is an input field Documents. When you select the Document Input Field, the Parameter Info is displayed.

The Parameter Info comprises of two sections:

1. Input Parameter

2. Output Parameter

Input Parameter

Input Parameter explains the type of input required for the selected field. It is specific to the input field within the task template.

Output Parameters

Output Parameters explains about the different outputs obtained from the task. It is specific to the whole task and not only for any one input field.

21.7.5.2 Editing Scenarios

You edit scenarios in the Workflow Assistant.

Procedure

1. In the *Scenarios* tab of the Workflow Assistant, choose (*More*) and select *Edit*.

The "Edit Scenario" screen appears.

2. In the *Edit Scenario* screen, make the required edits to the scenario by adding/removing the task templates/workflow templates or by modifying the input parameter values of the templates.
3. Choose *Save*.

   The "Save Scenario" dialog appears.
4. In the *Save Scenario* dialog, modify the name of the scenario as required and choose *Save*.

   The modifications to the scenario are saved and you return to the Home page of the Workflow Assistant.

21.7.5.3 Deleting Scenarios

You delete scenarios in the Workflow Assistant.

Procedure

1. In the *Scenarios* tab of the Workflow Assistant, choose (*More*) and select *Delete*.
2. Choose *Delete* in the warning that appears.

   The deleted scenario is no longer listed in the *Scenarios* tab of the Workflow Assistant.

21.7.5.4 Running Scenarios and Viewing Results

You run scenarios on BI data and view results in the Workflow Assistant.

Procedure

1. In the *Scenarios* view of the Workflow Assistant, choose (*More*) and select *Run* or *Run with Parameter*.

   Run with Parameter will open a dialog showing all input parameters of the scenario and you can change values or set missing values.

   > ⓘ Note
   >
   > The values set in this parameter dialog is not saved with the scenario, they are only used for the running instance.

   The scenario (tile or listed item) starts displaying the new status as Running or Pending. After the execution has completed, the status is updated to display the relevant value (`<Success/Partial Success/Failed/Pending/Error/Running with Error>`).

2. To view the results of the scenario (while it is running or after it has successfully run), choose ⋯ (*More*) and select *View Results*.

> **Note**
>
> You can select the View History option to check the results of a scenario's previous executions.

3. On the *Results* page, expand the results to view the execution and completion details of each workflow template and task template in the scenario. Once you have viewed the results, you can return to the main screen using the < (*Back*) button.

> **Note**
>
> You can select the Export option to save the scenario results in PDF format.

> **Note**
>
> 1. You can set a maximum time for a task to respond to an agent by adding the time (in seconds) against the key value task_time_out in the wfmanager_conf.properties file. By default, the key value task_time_out is set to 86400, that is, one day.
>
> 2. The task_time_out is set for all the agents in the Workflow Assistant.

21.7.5.5 Stopping Scenarios

You can stop a scenario while the execution of the task is still in progress.

Prerequisites:

You can proceed with the steps below only if a scenario is in Running or Pending state.

- In the Scenarios view, select *More* of the scenario.
- Choose Stop.

> **Note**
>
> The Stop option doesn't stop the scenario immediately. After you select the Stop option, the current task, that is being executed, is first completed and then the scenario is stopped. This means that only the pending tasks in the scenario will not be executed.

21.7.6 Understanding the States of Task Templates, Workflow Templates and Scenarios

Possible Artifact (Task Template/Workflow Template/Scenario) States with Descriptions

State	Description
Created (C)	When an artifact is created but not yet executed (run) even once.
Pending (P)	When an artifact is triggered for execution and is waiting in queue for its execution.
Running (R)	When an artifact is being executed.
Success (S)	When all the processed items are successfully executed. For example, the processed documents are refreshed successfully after the Refresh Document task. **Note** If even one workflow template in a scenario is not successful in execution, the overall scenario does not attain the state of 'Success'.
Partial Success (PS)	When only a few processed items are executed successfully. For example, when a few documents fail to refresh after the Document Refresh task, the state changes to Partial Success.
Failure (F)	When all the items are not executed successfully.
Error (E)	When an artifact encounters an error or exceptions during execution.
Running With Error (RE)	When an artifact encounters an error on the server, but continues to execute.
Not Executed	When a task template or workflow template in a scenario does not execute due to conditional parameter settings. For example, if the administrator chooses to set the condition of `<On Success>` between two workflow templates, due to which the flow of execution does not reach the next workflow template if the previous workflow template has failed. In such a case, the next and subsequent workflow templates remain in the `<Not Executed>` state.

Note

Here are the legends for the tables:

- TTS: Task Template Status
- WFTS: Workflow Template Status
- SS: Scenario Status

Status Matrix: Task Templates' Status and Resultant Workflow Template Status

TTS1	TTS2	TTS3	TTS4	TTS5	WFTS
S	S	S	E	NE	E (Error)
S	S	S	PS	NE	PS (Partial Success)
S	S	PS	F	NE	F (Failure)
S	PS	F	R	NE	R (Running)
S	E	NE	NE	NE	E (Error)
S	E	RE	NE	NE	RE (Running With Error)

The below matrix explain how the status of each workflow template impacts the overall status of the scenario.

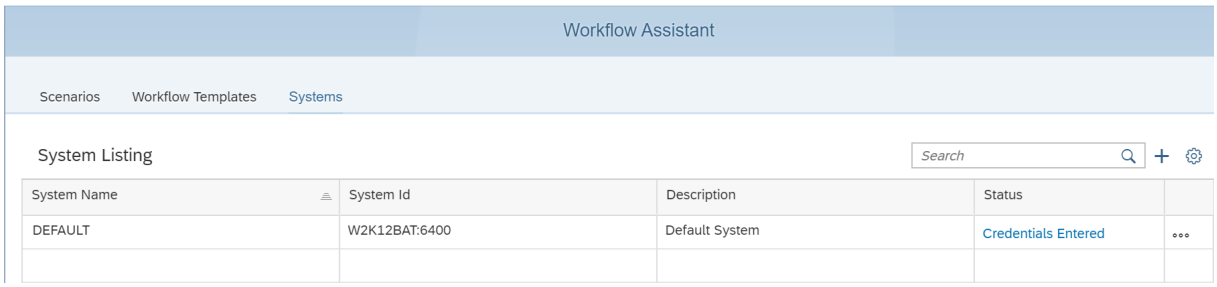
Status Matrix: Workflow Templates' Status and Resultant Scenario Status

WFTS1	WFTS2	WFTS3	WFTS4	WFTS5	SS
S	S	S	E	NE	E (Error)
S	S	S	PS	NE	PS (Partial Success)
S	S	PS	F	NE	F (Failure)
S	PS	F	R	NE	R (Running)
S	E	NE	NE	NE	E (Error)
S	E	RE	NE	NE	RE (Running With Error)

21.7.7 Working with Systems

Systems tab allows you to register multiple BI landscapes. *Systems* gives you access to your registered BI landscapes.

Snapshot of the *Systems* tab



You can perform the following actions in the *Sytems* tab:

- Add (register) a new system

  > → Remember
  >
  > It is mandatory to register your systems in this tab so that you can use these systems in other views such as *Scenarios* and *Workflow Templates*.

- Modify (edit or delete) an existing system
- Connect (or disconnect) with the system by entering your credentials (`User Name, Password, Authentication`)

  > ⓘ Note
  >
  > The system on which you have installed the Workflow Assistant appears listed as the "Default" system in the *Systems* tab. However, to connect with this landscape, you need to enter your credentials.

- Customize the columns displayed in the Systems view

21.7.7.1 Registering New BI System

To connect with your authorized BI System and to use the Workflow Assistant capabilities, it is essential to first register (add) BI systems in the Workflow Assistant.

Context

To register systems, follow the procedure given below:

Procedure

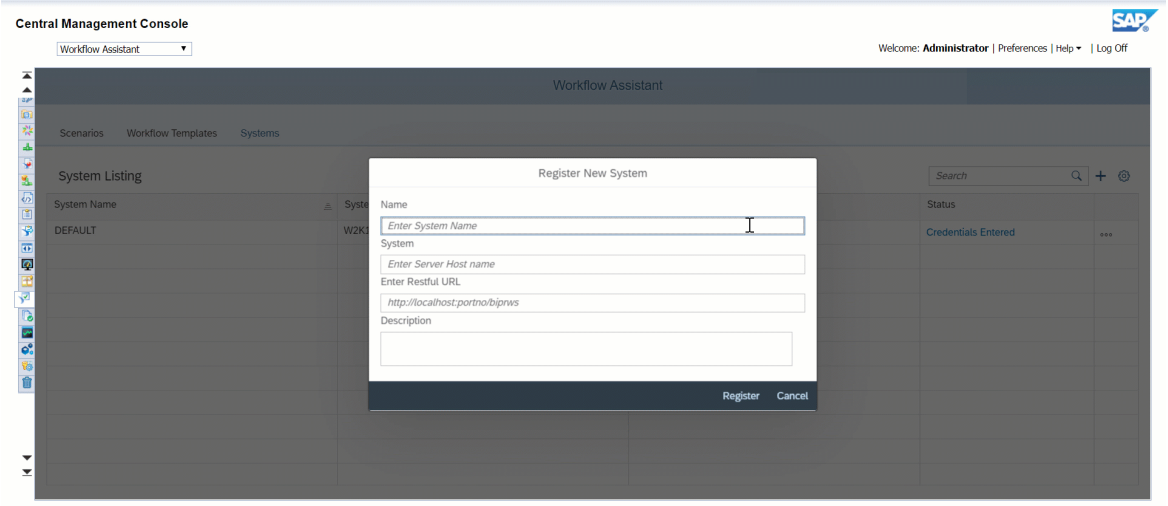
1. Log on to Workflow Assistant.
2. On the *Home* page, navigate to *Systems* tab.

   This view lists your available registered systems.
3. Choose the + (*Add*) icon.

   The "Register New System" dialogue appears.
4. For `<Name>`, enter an alias with which you can spot your system.
5. For `<System>`, enter the server host name or IP address which identifies your machine or your cluster of machines.
6. For `<RestFul URL>`, enter the RESTful Web services URL for the BI platform server. Optionally, you can add a `<Description>` for the system.
7. Choose *Register*.

> **Note**
>
> You can register the same BI system with different names, but it is recommended to have a BI system registered only once in the Systems view.

The registered system is added to your list of systems in the System Listing table.



21.7.7.2 Modifying Existing BI Systems

The Systems View allows you to modify your registered systems.

Context

To modify an existing system, follow the procedure given below:

Procedure

1. Log on to Workflow Assistant and navigate to *Systems* tab.
2. In the Systems view, choose ••• (*More*) → *Edit* for the listed system that you want to modify.

   The *Edit System* dialog appears.
3. Modify the `<Name>` (alias), `<System>`, `<RestFul URL>` or `<Description>` based on your requirements, and choose *Done*.

   The modifications start reflecting in the "System Listing" table.

> **Note**
>
> To delete a system, choose (*More*) → *Delete* for the listed system that you want to remove, and then confirm the deletion in the dialog which appears.

21.7.7.3 Connecting to Registered BI Systems

You can connect to your registered systems, using the `<Status>` field in the Systems Listed table. Connecting to BI system is essential for using your systems in the scenarios in Workflow Assistant.

Context

To connect to an added BI system, follow the procedure given below:

Procedure

1. Log on to Workflow Assistant and navigate to *Systems* tab.
2. Choose the flag string (*No Credentials Entered*) appearing in the `<Status>` field of the registered systems to which you are not yet connected.

   The "Enter Credentials" dialogue appears.
3. Enter your credentials for the BI system (based on authorization granted by your platform administrator): `<User Name>`, `<Password>` and `<Authentication>`. Then choose *Save*.

   The Workflow Assistant validates your credentials and updates the `<Status>` of your BI landscape to *Credentials Entered* if the validation is successful. Otherwise, an error message is displayed and the `<Status>` remains unchanged.

21.7.7.4 Customizing the Systems View

You can customize the appearance of the System Listing view by changing the visibility of fields (columns) in the view.

Context

To hide/show specific columns of the Systems view, follow the below procedure:

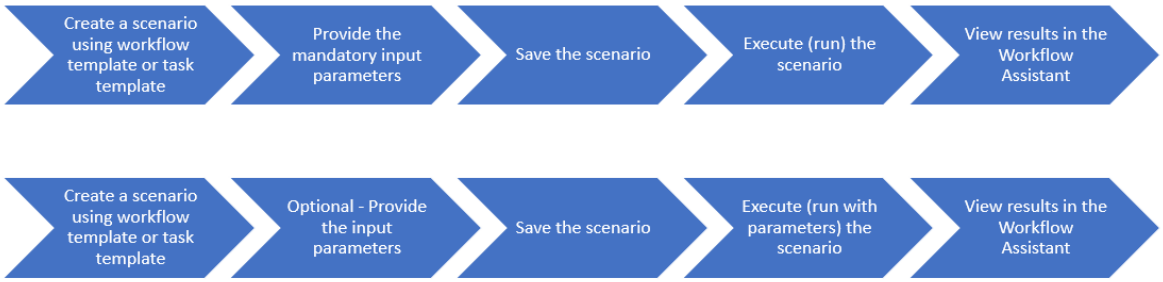
Procedure

1. Log on to Workflow Assistant and navigate to *Systems* tab.
2. Choose (*Settings*) and deselect the columns (field headers) that you wish to hide in the Systems Listing table.

   Your deselected columns no longer appear in the System Listing table.
3. To include a hidden column back into the view, choose *Settings* and select the required field headers again.

21.7.8 End-to-End Process Flow of the Workflow Assistant

See a visual representation.



21.8 Checking Log Files

This topic explains how you can check the log files of the Workflow Assistant.

Workflow Assistant

For Workflow Assistant, you should choose the trace level in the *WorkflowAssistant_Trace.ini* file at `<INSTALLDIR>\AdminConsole\WorkflowAssistant`. Trace files can also be configured using **_Trace.ini** file by setting the following environment variables:

- `BO_TRACE_CONFIGDIR`, to set the folder name of configuration files for logs, for example: `C:\BOTraces\config`
- `BO_TRACE_CONFIGFILE`, to set the name of the configuration file, for example `BO_trace.ini`
- `BO_TRACE_LOGDIR`, to set the folder name for logs, for example: `C:\BOTraces`

> **Note**
>
> The `INI` file name is case-sensitive.

Create the `BO_trace.ini` configuration file as follows:

```
sap_log_level = log_info;
sap_trace_level = trace_debug;
```

You can check logs by default in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`.

22 Recycle Bin

22.1 Recycle Bin

About Recycle Bin

Recycle Bin is a new application in the CMC. When the user deletes an item from the BOE system, it is moved to the Recycle Bin, where it is temporarily stored until the Recycle Bin is emptied. This gives the user the opportunity to recover accidentally deleted reports/folders and restore them to their original locations.

With the Recycle Bin application, the administrator can:

- Initiate restoration of any deleted item (such as reports and folders)
- Permanently delete items from the Recycle Bin
- Perform auto-cleanup of the Recycle Bin

If Recycle Bin is enabled, you can recycle the following infoobject types:

- Personal folder content
- Events
- Calendars
- Public folder content
- Universes
- Connections
- Public categories
- Personal categories
- Inboxes
- Profiles
- Custom roles

22.1.1 Restoring an Item from the Recycle Bin

Context

The Recycle Bin displays a list of deleted items. In order to restore an item from the recycle bin, proceed as follows:

Procedure

1. Log on to the CMC.
2. From the *Manage* pane on the CMC home page, choose *Recycle Bin*.
3. Right-click on the item you want to restore, and select *Restore* from the context menu.
4. Choose *OK*.

   You can navigate to the location of the restored item to confirm the restore operation.

> ### Note
>
> If you restore an item from the Recycle Bin and another item with the same name already exists in the restore location, the item is saved in the restore location with the following name: "<item name> restored(1, 2, ...)".
>
> When the parent folder of an item in the Recycle Bin is deleted, the parent folder is recreated when the item is retored. However, the parent folder will only contain the item(s) that is restored from the Recycle Bin.
>
> You cannot open/navigate an item from within the Recycle Bin.
>
> If you delete an item from a folder and later admin restrics the modification rights of that folder, when you try to restore the item back to the original folder, the item is still restored to the original folder.

Results

You have now successfully restored an item from the Recycle Bin.

22.1.2 Permanently Deleting Items from the Recycle Bin

As an administrator, you have the right to permanently delete selected items from the Recycle Bin or to empty the Recycle Bin.

Context

In order to permanently delete items from the Recycle Bin, proceed as follows:

Procedure

1. Log on to the CMC.
2. From the *Manage* pane on the CMC home page, choose *Recycle Bin*.
3. Right-click on the item you want to delete, and select *Delete* from the context menu.
4. Choose *OK*.

Results

You have now successfully deleted an item from the Recycle Bin.

22.1.3 Enabling Auto-Cleanup for the Recycle Bin

You can run auto-cleanup of the recycle bin periodically.

Context

To enable auto-cleanup of the recycle bin, proceed as follows:

Procedure

1. Log on to the CMC.
2. From the *Manage* pane on the CMC home page, choose *Applications*.
3. From the *Applications* page, choose *Recycle Bin* application.

The *Properties: Recycle Bin* dialog box opens.

4. Select the checkbox and specify (in days) how long the system should wait before auto-cleaning a deleted item.
5. Choose *Save & Close*.

Results

You have now successfully enabled auto-cleanup for the Recycle Bin.

23 Auditing

23.1 Overview

Auditing allows you to keep a record of significant events on servers and applications, which helps give you a picture of what information is being accessed, how it's being accessed and changed, and who is performing these operations. This information is recorded in a database called the Auditing Data Store (ADS). Once the data is in the ADS, you can design custom reports to suit your needs. You can look for sample universes and reports on the SAP Community http://community.sap.com/.

For the purposes of this chapter, an auditor is a system responsible for recording or storing information on an event, and an auditee is any system responsible for performing an auditable event. There are some circumstances where a single system can perform both functions.

How Auditing works

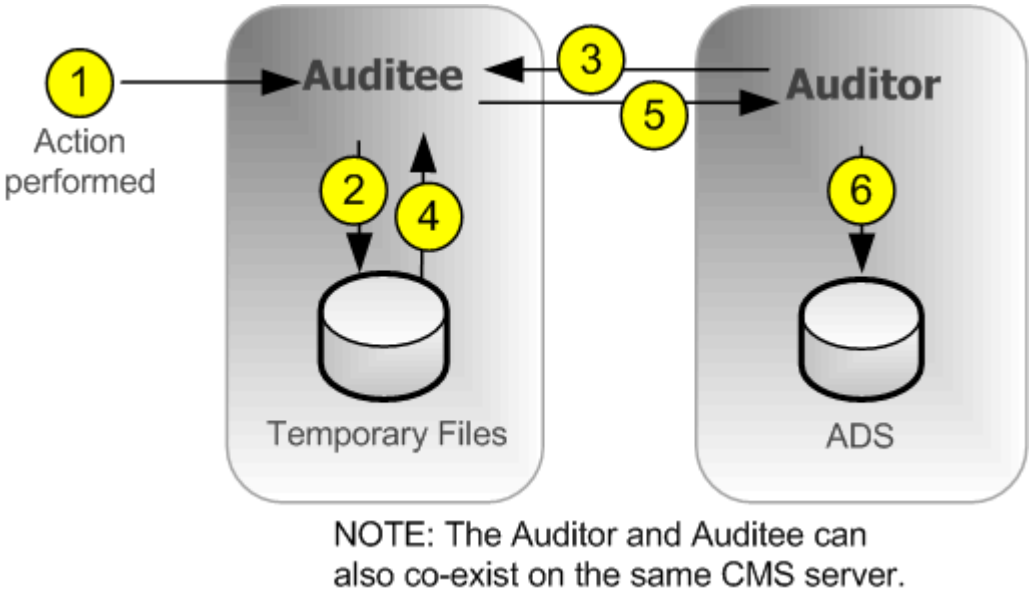
The Central Management Server (CMS) acts as the system auditor, while each server or application that triggers an auditable event acts as an auditee. When an audited event is triggered, the auditee will generate a record and store it in a local temporary file. At regular intervals, the CMS communicates with the auditees to request these records and writes the data to the ADS.

The CMS also controls the synchronization of auditing events that occur on different machines. Each auditee provides a timestamp for the auditing events that it records. To ensure that the timestamps of events on different servers are consistent, the CMS periodically broadcasts its system time to the auditees. The auditees then compare this time to their internal clocks. If differences exist, they correct the time recorded for subsequent auditing events.

Depending on the type of auditee, the system uses one of the following workflows to record the events.

Server auditing

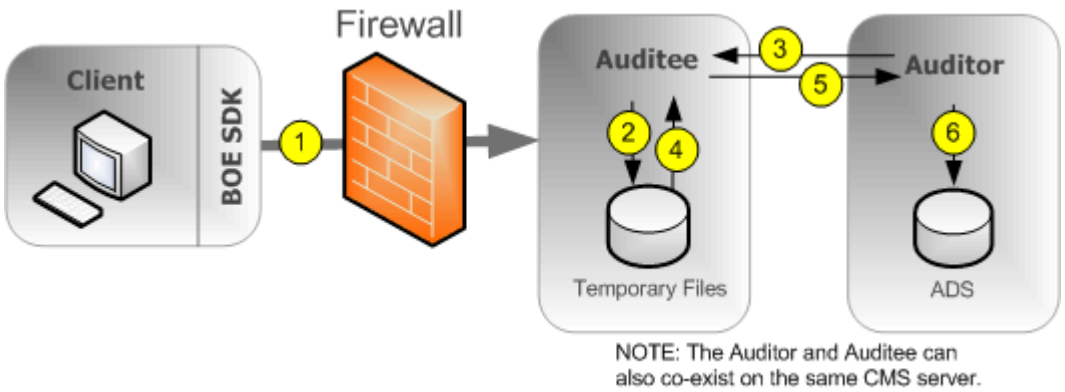
In cases of server generated events, the CMS can act as both Auditee and Auditor.



1. An auditable event is performed by the server.
2. The auditee writes events in a temporary file. Steps 1 and 2 can occur multiple times before step 3.
3. At regular intervals, the auditor polls the auditee and requests a batch of auditing events.
4. The auditee retrieves the events from the temporary files.
5. The auditee transmits the events to the auditor.
6. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

Client logon auditing for clients connecting through CORBA

This includes applications such as SAP BusinessObjects Web Intelligence.



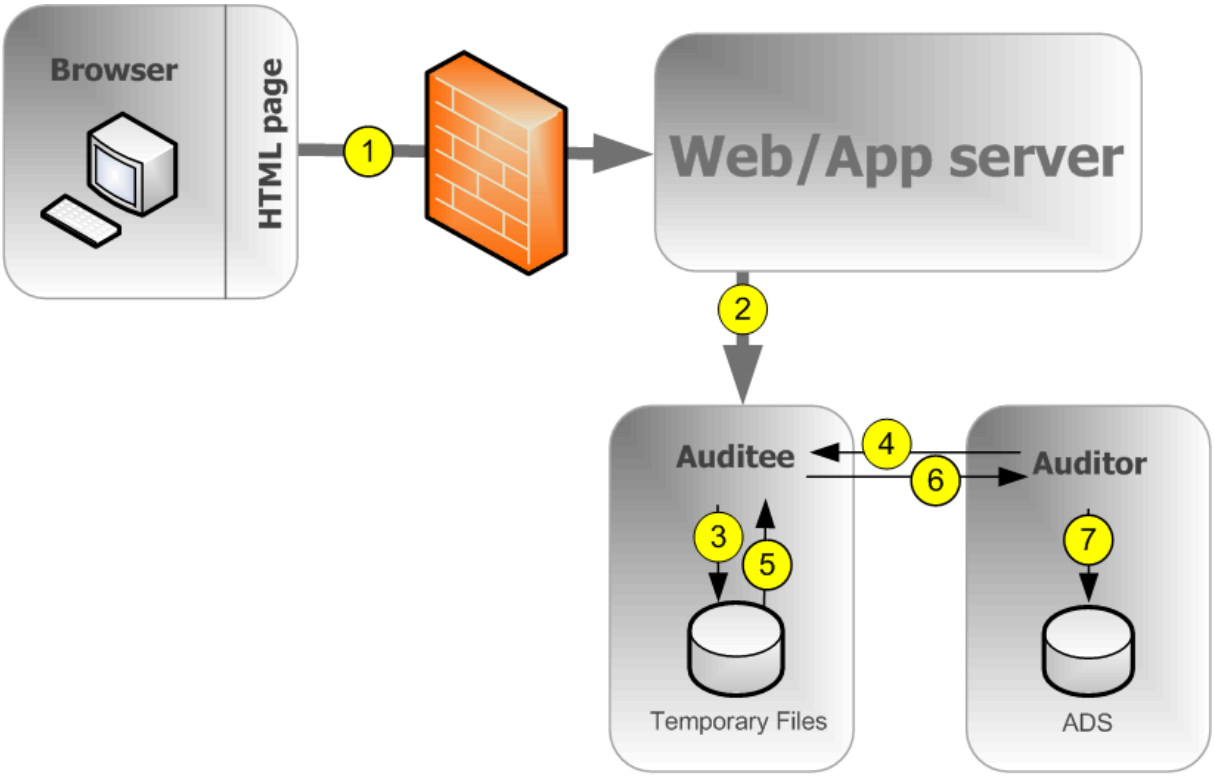
1. The client connects to the CMS, which will act as the auditee. The client provides its IP address and machine name, which the auditee then verifies.

> **Note**
>
> A port should be opened in the firewall between the client and CMS. More details on firewalls can be found in the security chapter of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

2. The auditee writes events in a temporary file. Steps 1 and 2 can occur multiple times before step 3.
3. At regular intervals, the auditor polls the auditee and requests a batch of auditing events.
4. The auditee retrieves the events from the temporary files.
5. The auditee transmits the events to the auditor.
6. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

Client logon auditing for clients connecting through HTTP

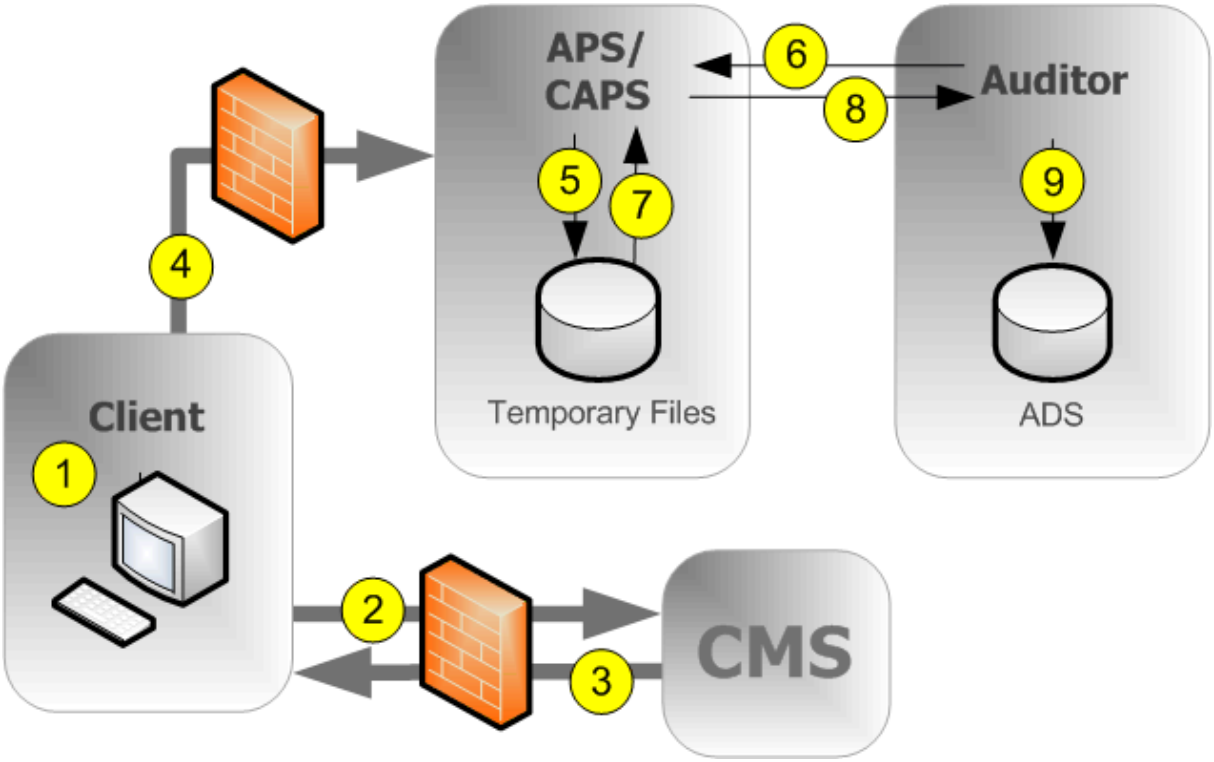
This includes online applications such as BI launch pad, Central Management Console, SAP BusinessObjects Web Intelligence, and so on.



1. The browser connects to the web application server, and logon data is submitted to the web application server.
2. The BI platform SDK submits the logon request to the auditee (CMS), along with the IP address and name of the browser machine.
3. The auditee writes events in a temporary file. Steps 1 to 3 can occur multiple times before step 4.
4. At regular intervals, the auditor polls the auditee and requests a batch of auditing events.
5. The auditee retrieves the events from the temporary files.
6. The auditee sends events to the auditor.
7. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

Non-Logon auditing for clients connecting through CORBA

This workflow applies to auditing SAP BusinessObjects Web Intelligence events when connecting through CORBA.



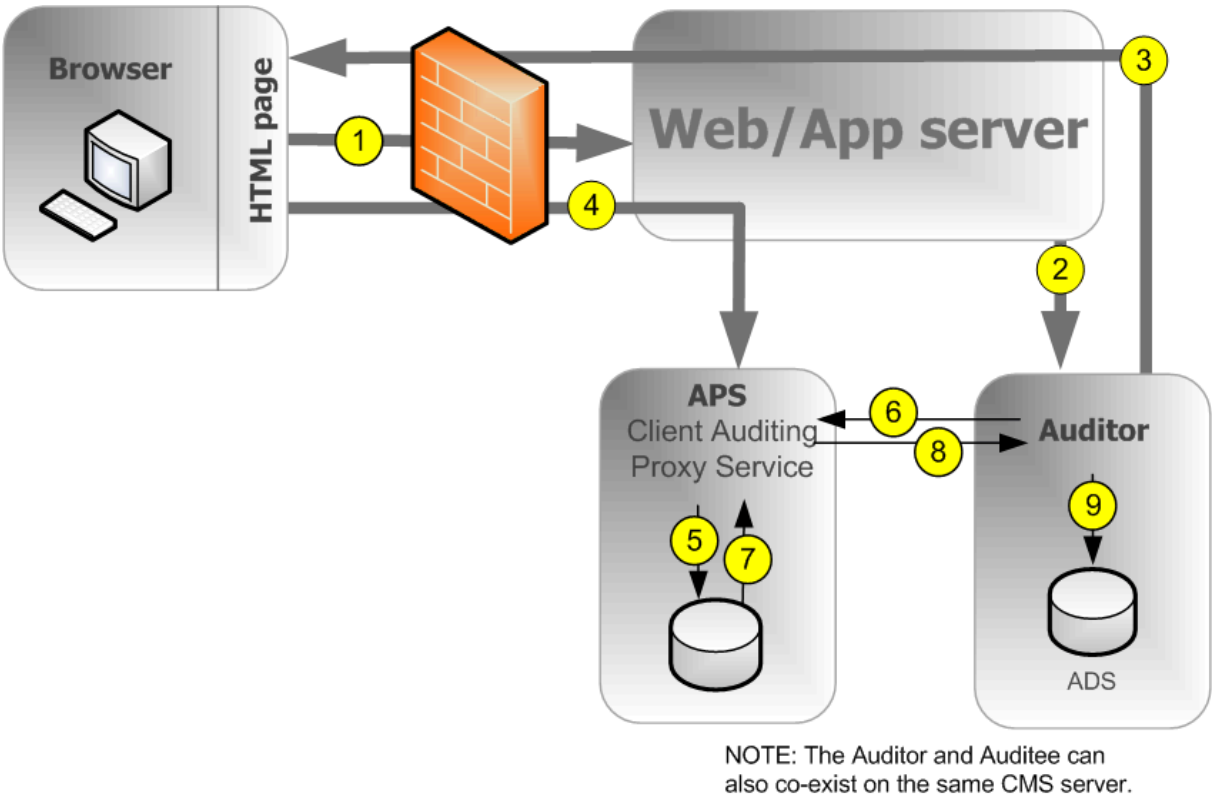
1. The user performs an operation that may be audited.
2. The client contacts the CMS to check if the operation is configured to be audited.
3. If the action is set to be audited, the CMS communicates this information to the client.
4. The client sends the event information to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server.

   > **Note**
   >
   > A port in the firewall should be opened between each client and any Adaptive Processing Servers that hosts a CAPS, and also between each client and the CMS. More details on firewalls can be found in the security chapter of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

5. The CAPS writes events in a temporary file. Steps 1 to 5 can occur multiple times before step 6.
6. At regular intervals, the Auditor polls the CAPS and requests a batch of auditing events.
7. The CAPS retrieves the events from the temporary files.
8. The CAPS sends the event information to the auditor.
9. The auditor writes events to the ADS and signals the CAPS to delete the events from the temporary files.

Non-login auditing for clients connecting through HTTP

This workflow applies to auditing SAP BusinessObjects Web Intelligence events (except for logon events) when connecting through HTTP.



1. The user initiates a potentially auditable event. The client application contacts the web application server.
2. The web application checks to see if the event is configured to be audited.

   > **Note**
   >
   > The diagram shows the Auditor CMS being contacted, but any CMS in the cluster can be contacted for this information.

3. The CMS returns the audit configuration information to the web application server, which passes this information back to the client application.
4. If the event is configured to be audited, the client sends the event information to the web application server, which passes it to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server (APS).
5. The CAPS writes events in a temporary file. Steps 1 to 5 can occur multiple times before step 6.
6. At regular intervals, the auditor polls the CAPS and requests a batch of auditing events.
7. The CAPS retrieves the events from the temporary files.
8. The CAPS sends the event information to the auditor.
9. The auditor writes events to the ADS and signals the CAPS to delete the events from the temporary files.

Clients that support auditing

The following client applications support auditing:

- BI Launch Pad (BILP)
- Central Configuration Manager (CCM)
- Central Management Console (CMC)
- OpenDocument
- Information Design Tool (IDT)
- Translation Management Tool (TMT)
- Web Intelligence Rich Client (WIRC)
- Lumira Desktop Application (Discovery)
- Lumira Designer Application

> **Note**
>
> At least one instance of CAPS must be running in order to collect auditing events from the clients listed above.

Clients not listed above do not directly generate events, but some actions performed by the servers as a result of client application operations can be audited.

Auditing consistency

In most cases, where auditing is properly installed, configured, secured, and correct versions of all client applications are used, auditing will properly and consistently record all indicated system events. It is important to keep in mind, however, that certain system and environment conditions can adversely affect auditing.

There is always a delay between the time an event occurs and its final transfer to the ADS. Conditions such as the unavailability of the CMS or auditing database or loss of network connectivity can increase these delays.

As a system administrator, you should work to avoid any of the following conditions, which could result in incomplete auditing records:

- A drive where auditing data is stored reaches maximum capacity. You should ensure plenty of disk space is available for your auditing database and auditee temporary files.
- An auditee server is improperly removed from the network before it can transmit all audit events. You should ensure that when removing a server from the network, sufficient time is allowed for audit events to post to the auditing database.
- The deletion or modification of auditee temporary files.
- A hardware or disk failure.
- Physical destruction of an auditee or auditor host machine.

There are also some conditions where audit events may be prevented from reaching the CMS-Auditor. These can include:

- Users with older client versions.
- Transmission of auditing information may be blocked by improperly configured firewalls.

> **Note**
>
> Events generated by client applications contain information submitted from the client side, in other words outside the trusted area of the system. Therefore under some conditions this information may not be as reliable as information recorded by the system servers.

> **Note**
>
> If you want to remove a server from your deployment, you should first disable that server but keep it running and connected to your network until all the events in the temporary files have had a chance to transfer to the auditing database. The server's *Current Number of Auditing Events in the Queue* metric will show how many auditing events are waiting to be transferred. When this metric reaches zero, you can stop the server. The location of the temporary files is defined by the `%DefaultAuditingDir%` placeholder for that node. See the Server Administration chapter for more details on placeholders.

> **Note**
>
> If you are going to use Client Auditing it is recommend that you create a dedicated Adaptive Processing Server for the Client Auditing Proxy Service. This will ensure your best system performance. To increase your system's fault tolerance you may also want to consider running the CAPS on more than one APS.

Related links

Server and node placeholders [page 1102]

23.2 CMC Auditing page

The *Auditing* page in the CMC has the following areas:

- *Status Summary*
- *Set Events*
- *Set Event Details*
- *Configuration*

23.2.1 Auditing Status

The Auditing *Status Summary* shows a set of metrics that help you optimize your auditing configuration and alert you to any issues that might affect the integrity of your auditing data. The status summary is at the top of the *Auditing* page in the Central Management Console.

The summary will also display warnings under the following circumstances:

- The connection to the Auditing Data Store (ADS) database is unavailable.
- There is no running or enabled Client Auditing Proxy Service, which prevents client events from being collected.
- An auditee has events that could not be retrieved (the server or servers affected will be identified). This usually indicates a server was not properly stopped or shut down and still has events in the temporary files.

> **Note**
>
> The status summary metrics are marked green, yellow, or red to indicate the health of the auditing feature.

Auditing Status metrics

Metric	Details
ADS Last Updated on	The date and time the auditor CMS last finished polling the auditees for their auditing events.
Auditing Thread Utilization	The percentage of the polling cycle the auditor CMS spends collecting data from auditees, the remainder is time spent resting between polls. If this reaches 100% the figure will be displayed in yellow, and means the auditor is still collecting data from the auditees when the next poll is due to begin. This may cause delays in the events reaching the ADS. If this is happening frequently or persistently, it is recommended that you either update your deployment to allow the ADS database to receive data at a higher rate (faster network connections or more powerful database hardware for example), or decrease the number of auditing events your system tracks.
Last Polling Cycle Duration	Duration of the last polling cycle in seconds. This indicates the maximum delay for event data to reach the ADS during the previous polling cycle. • If under 20 minutes (1200 seconds), the figure will appear on a green background. • If between 20 minutes and 2 hours (7200 seconds), it will appear on a yellow background. • If over 2 hours, it will appear on a red background. If this state persists and you consider the delay too long, it is recommend you either update your deployment to allow the ADS database to receive data at a higher rate (faster network connections or more powerful database hardware for example), or decrease the number of auditing events your system tracks.

Metric	Details
CMS Auditor	The name of the CMS currently acting as auditor.
ADS Database Connection Name	The name of the database connection currently used by the auditor CMS to connect to the Auditing Data Store (ADS). For SQL Anywhere, SQL Server, and SAP HANA servers, this will be the name of the ODBC connection. For other database types it will be the database name and connection port, followed by the server name.
ADS Database User Name	The user name the auditor CMS is using to log in to the ADS database.

23.2.2 Configuring Auditing events

The CMC Auditing page can be used to activate auditing and select which events will be audited across your entire system.

If you are not interested in certain events or event details, you can leave them unselected to gain additional system performance.

> ⓘ Note
>
> Audit events are pushed into the Audit database in batch mode as opposed to one event at a time.The batch size is currently set to 1000 audit events.

> ⓘ Note
>
> If you chose not to configure your ADS connection when you installed the BI platform, you will need to set up a connection to the database before you configure your auditing events. Without a connection, events will still be collected, but once connected, the events will be written to the ADS. To turn off auditing the level should be set to off. See *Auditing Data Store configuration settings.*

23.2.2.1 To Configure Auditing Events

Context

To configure the auditing events, perform the following steps:

Procedure

1. In the Central Management Console, select the *Auditing* tab.
   The *Auditing* page appears.
2. Set the *Set Events* slider to the desired auditing level, where each auditing level corresponds to a specific metric value.
   - *Off* - 1
   - *Minimal* - 2
   - *Default* - 3
   - *Complete* - 4
   - *Custom* - 0

   The following table shows the different settings for the slider and the events captured at each level.

Auditing Level	Events captured
Off	None
Minimal	• Logon • Logout • Rights Modification • Custom Access Level Modified • Auditing Modification
Default	*Minimal* events, plus: • View • Refresh • Prompt • Create • Delete • Modify • Save • Search • Edit • Run • Deliver
Complete	*Minimal* and *Default* events plus: • Trigger

Auditing Level	Events captured
	• Drill Out of Scope. • Page Retrieved • Promotion Management Configuration • Rollback • VMS Add • VMS Retrieve • VMS Check-in • VMS Check-out • VMS Export • VMS Lock • VMS Unlock • VMS Delete • Cube Connection • MDAS Session **Note** You can view more events when the add-ons are installed.
Custom	You select a custom set of events.

Note

When the *Set Events* is set as *Default*, the *Auditing Level* value is 3.

When the *Set Events* is set as *Off*, the *Auditing Level* value changes from 3 to 1.

3. Select *Custom*, click the events you want to capture in the list below the *Set Events* slider.
4. Click the optional details under *Set Event Details* that you want to record with the events, recording fewer details increases system performance.

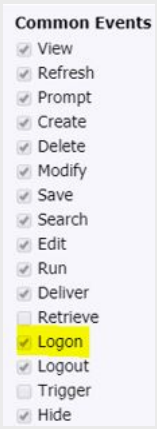
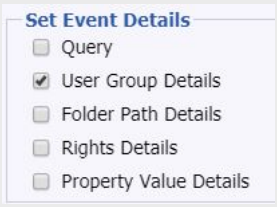
Detail	Description
Query	If set, *Query* event detail (Detail ID 25) is recorded for any event that queries a database.
Folder Path Details	If set, the following details are captured: • *Object Folder Path (Detail ID 71)* • *Top Folder Name (Detail ID 72* • *Container folder path (Detail ID 64)*
Rights Details	If set, the following details are captured: • *Right Added (Detail ID 55)* • *Right Removed (Detail ID 56)* • *Right Modified (Detail ID 57)*
User Group Details	If set, the following details are captured: • *User Group Name (Detail ID 16)* • *User Group ID (Detail ID 15)*

Detail	Description
Property Value Details	If set, the *Property Value* event detail (Detail ID 29) is captured when the properties of an object are updated. This is generated only for CMC, BI launch pad, or SharePoint events.

5. Click *Save*.

> **Note**
>
> For client auditing, it takes up to 2 minutes after the changes are made before the system starts recording data for any new events. Make sure that you allow for this delay when implementing changes to the system.

23.2.2.2 Enhanced Event Detail Recording in Audit Detail Table

> **Note**
>
> - You should have sufficient knowledge regarding the CMC Auditing page [page 818], especially *Common Events, Set Event Details, User Group Details*, and *Logon*, in order to consume the information provided below.
> - *Logon* is an event that provides details of a user accessing the application.
>
> 
>
>
> - *User Group Details* provides information about the user groups associated with a user for each event.
>
> 
>

The recording of user group details in the AUDIT_EVENT_DETAIL table is partially dependent on the selections made under *Common Events* and *Set Event Details* in the Auditing page. Consider a scenario where you have selected *Logon* but not the *User Group Details* in the *Auditing* page. In this scenario, the user group details are

still recorded for the *Logon* event in the AUDIT_EVENT_DETAIL table. See the table below to understand the behavior in BI 4.2 Support Package 5.

Logon	User Group Details	Behavior
Selected	Selected	User Group details are recorded for all the events selected under Common Event.
Selected	Not selected	User Group details are recorded only for Logon events.
Not selected	Not selected	User Group details are not recorded.
Not selected	Selected	User Group details are recorded for all selected events except Logon events.

23.2.3 Auditing Data Store Configuration Settings

If you chose not to set up an auditing database when you installed the BI platform, or you want to change the database location or settings, you can use the following steps to configure the connection to the ADS.

This is also where you can configure how long auditing events will be retained in the database.

If you have performed an upgrade from a previous version of SAP BusinessObjects Enterprise XI 3.x and have installed version 3.x of Business Objects Metadata Manager (BOMM), it is recommended to configure the ADS to use the same database or tablespace as BOMM.

> ⓘ Note
>
> If you are using an existing DB2 9.7 Workgroup as the auditing database, then ensure that the database account is configured to have a page size over 8 KB.

23.2.3.1 To configure your Auditing Data Store database settings

Procedure

1. On the Central Management Console, select the *Auditing* tab.
2. In the *Configuration* area, under the *ADS Database* heading, select the database type you have set up for your auditing data.
3. In the *Connection Name* field, enter the name of the connection you have configured for the auditing database.

Database type	Connection name
IBM DB2	service name
Microsoft SQL Server	ODBC DSN
MySQL	`<serverhostname>,<port>,<databasename>`
Oracle	TNS service name
SAP HANA	ODBC DSN
SAP MaxDB	`<serverhostname>,<port>,<databasename>`
Sybase Adaptive Server Enterprise	service name
Sybase SQL Anywhere	ODBC DSN

   a. If you are using a Microsoft SQL database with Windows authentication, enable the *Windows Authentication* option.

4. In the *User Name* and *Password* fields, enter the user name and password you want the auditor CMS to use when logging onto the database.
5. In the *Delete Events Older Than (Days)* field, enter the number of days you want information to remain in the database. (Minimum value 1, maximum value 109,200.)

   > ⚠ Caution
   >
   > Data older than the number of days set here will be permanently deleted from the ADS; it cannot be recovered. You may want to consider periodically moving records to an archive database if you want to maintain long-term records.

6. In the event the database connection is lost, if you want to manually reconnect the auditor-CMS to the database, de-select the *ADS Auto Reconnect* option.

   > ⓘ Note
   >
   > If this is unchecked, you will need to manually re-establish a connection to the ADS if the connection is lost. This can be done by restarting the CMS, or enabling *ADS Auto Reconnect*. Events will be recorded and remain stored in the temporary files until the ADS is reconnected.

7. Click *Save*.
8. Restart all CMSs in the cluster.

   > ⓘ Note
   >
   > The *Status Summary* at the top of the page shows the current ADS values, which can be different from the values in the *ADS Database* section until the CMSs are restarted.

23.3 Audit events

The following table shows all the auditing events in the system, and gives a brief description for each. A list of the service types that create the events follows.

Event	
Auditing Modification Description, and servers and clients that generate the event type	The system's auditing settings are modified. • Central Management service
Create	A new object is added to the system. • BI Commentary Service • Central Management Service • Crystal Reports Viewing and Modification Service • Desktop Intelligence • Information Engine Service • Lifecycle management • Web Intelligence • Web Intelligence Common Service • Description, and servers and clients that generate theWeb Intelligence Core Service • Web Intelligence Processing Service
Cube Connection	An OLAP Cube Connection operation is performed. • Multi-Dimensional analysis service • Analysis Applications
Custom Access Level Modified	Information for privileges is modified. • Central Management service
Delete	An object is removed from the system. • BI Commentary Service • Central Management service • Lifecycle Management service
Deliver	An object is sent/delivered to a destination. • Authentication Update Scheduling Service • Central Management Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Desktop Intelligence • Destination Delivery Scheduling Service • Platform Search Scheduling Service • Probe Scheduling Service • Program Scheduling Service • Security query scheduling service • Users and Groups Import Scheduling Service

Event	
	• Web Intelligence Scheduling and Publishing Service
Drill out of scope	A user of a Web Intelligence document has drilled down to a detail level outside the report's pre-loaded data. • Web Intelligence • Web Intelligence Processing Service • Web Intelligence Common Services • Web Intelligence Core Services • Information Engine Service
Edit	The content of an object is changed. • BI Workspaces Application • Desktop Intelligence • Information Engine Service • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
LCM Configuration	The configuration details of Lifecycle Management Console (LCM) are changed. • Lifecycle Management
Logon	A user logs onto the system. • Central Management service
Logout	A user logs out of the system. • Central Management service
Modify	The file properties of an object are changed. • Web Intelligence • Lifecycle Management • Central Management service • BI Commentary Service
MDAS Session	A multi-dimensional analysis services operation is performed. • Multi-Dimensional analysis service
Page Retrieved	An SAP BusinessObjects Web Intelligence client retrieves additional information from the repository. • Web Intelligence processing service • Web Intelligence Common Services • Web Intelligence Core Services • Information Engine Service
Prompt	Information is entered for an object prompt.

Event	
	• Crystal Reports Cache Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Desktop Intelligence • Information Engine Service • Live Office • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
Refresh	The data in an object is updated from the database at a user's request. • Crystal Reports Cache Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Desktop Intelligence • Information Engine Service • Live Office • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
Retrieve	An object is retrieved from the repository. • Central Management service • Desktop Intelligence
Rights Modification	The security information is changed for a user, group, or object. • Central Management service
Rollback	LifeCycle Manager is used to revert an object to a previous version. • Lifecycle Management
Run	A job is run. • Authentication update scheduling service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Desktop Intelligence • Destination Delivery Scheduling Service • LCM Scheduling Service • Lifecycle management • Platform Search Scheduling Service • Probe Scheduling Service

Event	
	• Program Scheduling Service • Publication Scheduling Service • Replication Service • Security query scheduling service • Users and Groups Import Scheduling Service • Visual Difference Scheduling Service • Web Intelligence Scheduling and Publishing Service
Save	An object is saved after being updated or changed. • Analysis edition for OLAP • Crystal Reports Cache Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Crystal Reports Viewing and Modification Service • Desktop Intelligence • Information Engine Service • Lifecycle management • Multi-Dimensional Analysis Service • SAP BusinessObjects Mobile • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
Search	A search is performed. • Search service • Explorer • Lifecycle management
Trigger	A file event is triggered. • Event service • Central Management service
View	An object is Viewed. • Analysis Applications • Analysis edition for OLAP • BI launch pad • BI Workspaces Application • BI Commentary Service • CMC • Crystal Reports Cache Service • Crystal Reports Viewing and Modification Service • Desktop Intelligence • Information Engine Service • Open Document

Event	
	• SAP BusinessObjects Mobile • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
VMS Add	An object is added to the LCM Version Management System. • Lifecycle Management
VMS Check in	An object is checked into the LCM Version Management System. • Lifecycle Management
VMS Check out	An object is checked out of the LCM Version Management System. • Lifecycle Management
VMS Export	A resource is exported from the VMS. • Lifecycle Management
VMS Lock	A resource in the VMS is locked. • Lifecycle Management
VMS Unlock	A resource in the VMS is unlocked. • Lifecycle Management
VMS Retrieve	An object is retrieved from the LCM Version Management System. • Lifecycle Management
VMS Delete	An object is deleted from the LCM Version Management System. • Lifecycle Management

Events by Service-type

Service type	Event types generated
Analysis Applications	• View • Cube connection
Authentication Update Scheduling Service	• Deliver • Run
Fiorified BI Launch Pad	View

Service type	Event types generated
BI Commentary Service	• Create • Delete • View • Modify • Hide
Central Management Service	• Auditing Modification • Create • Custom Access Level Modified • Delete • Deliver • Logon • Logout • Modify • Retrieve • Rights Modification • Trigger
Central Management Console	View
Crystal Reports Scheduling Service	• Deliver • Prompt • Refresh • Run • Save
Crystal Reports Cache Service	• Prompt • Refresh • Save • View
Crystal Reports for Enterprise Scheduling Service	• Deliver • Prompt • Refresh • Run • Save
Crystal Reports Scheduling Service	• Deliver • Prompt • Refresh • Run • Save
Crystal Reports Viewing and Modification Service	• Create • Save • View

Service type	Event types generated
Desktop Intelligence (client)	• Deliver • Prompt • Retrieve • Run
Desktop Intelligence scheduler process	• Deliver • Run
Destination Delivery Scheduling Service	• Deliver • Run
Event Service	Trigger
Information Engine Service	• Create • Drill out of scope • Edit • Page retrieved • Prompt • Refresh • Save • View
LCM Scheduling Service	Run
LCM service	• Create • Delete • LCM configuration • Modify • Rollback • Run • Save • VMS Add • VMS Checkin • VMS Checkout • VMS Delete • VMS Export • VMS Lock • VMS Retrieve • VMS Unlock • Search
Live Office	• Prompt • Refresh
Multi-Dimensional Analysis Service	• Cube Connection • MDAS Session • Save

Service type	Event types generated
OpenDocument	View
Platform Search Scheduling Service	• Deliver • Run
Platform Search Service	Search
Probe Scheduling Service	• Deliver • Run
Program Scheduling Service	• Deliver • Run
Publication Scheduling Service	Run
Replication Service	Run
SAP BusinessObjects Design Studio version 1.3 and later	• Logon • Logoff
Security Query Scheduling Service	• Run • Deliver
Users and Groups Import Scheduling Service	• Run • Deliver
Visual Difference Scheduling Service	Run
Web Intelligence Application	• Create • Drill out of scope • Edit • Modify • Prompt • Refresh • Save • View
Web Intelligence Common Service	• Create • Drill out of scope • Edit • Page retrieved • Prompt • Refresh • Save • View
Web Intelligence Core Service	• Create • Drill out of scope • Edit • Page retrieved

Service type	Event types generated
	• Prompt • Refresh • Save • View
Web Intelligence Processing Service	• Create • Drill out of Scope • Edit • Page Retrieved • Prompt • Refresh • Save • View
Web Intelligence Scheduling and Publishing Service	• Deliver • Run

Event properties and details

Each event that is recorded by the BI platform includes a set of event properties and details.

Event properties will always be generated with an event, although some may not have values if the information is not applicable to a specific event. In the ADS, event properties are included in the table that stores the event, so they can be used to sort or group events when you create reports.

Event details record additional information about the event that is not included in the event's properties. If an event detail is not relevant to a specific event, that event detail will not be generated. There is a set of common event details that can be generated for all event types when they are relevant. There are also sets of additional event details which are generated for specific event types. For example, Prompt events record the values entered for the prompt in an event detail, but no other event type generates a prompt value event detail. In the ADS, details are stored on a separate table which is linked to the parent event.

In some cases, event details can contain multiple values. These details can be grouped using the bunch ID. See the related topic for more information about bunch IDs.

Any multilingual data (such as object or folder names) will be recorded in the default language for the locale of the auditor CMS.

Related Information

Auditing Data Store Tables [page 1111]

23.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> **Note**
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> **Note**
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

Event Property	Description
Event_ID	A unique identifier for the event.
Client_Type_ID	Identifier for the type of application that performed the event
Service_Type_ID	Shows the ID of the type of service or application that triggered the event.
Start_Time	The start date and time when the event started (in GMT).
Duration	Duration of the event in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Session_ID	ID of the session during which the event was triggered.
Event_Type_ID	Type of event (for example, 1002 for view).
Status_ID	Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events.
Object_ID	CUID of the object affected (if applicable). CUID of the alerting event for Trigger events. **Note** All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need

Event Property	Description
	to use the Object_Name property to differentiate these objects.
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast`
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`.
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`.
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

> **Note**
>
> The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.

Event Detail	ID	Description
Parent Document ID	12	• For a document instance: the CUID of the parent document. • For parent documents: its own CUID.
Universe ID	13	CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used.
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.

Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

View

User viewed a document / object.

- Event Type ID: 1002

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

> **Note**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. **Note** For View on Demand Crystal Reports this will be set to 0.
Number of Rows	63	The number of records the database server returned. **Note** For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.
Publication Instance ID	37	ID of this instance of the publication. Only applicable to publishing workflows.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents.

Prompt

A value was entered for a prompt.

- Event Type ID: 1004

Event Detail	ID	Description
Prompt name	26	The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a

Event Detail	ID	Description
		document or object, and they will be grouped.
Prompt value	27	The value entered for a prompt. A separate detail will be generated for each value entered. These can be grouped together and related back to the prompt name.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).
Publication Instance ID	37	ID of this instance of the publication. Only applies to publishing workflows.
Name at Design Time	90	The name of the Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

Create

User created an object.

- Event Type ID: 1005

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Overwrite	21	Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable.
Description	24	Records any information in the document or object's description field.

Delete

User deleted an object.

- Event Type ID: 1006

Modify

User modified a file property or the file properties of an object.

- Event Type ID: 1007

Event Detail	ID	Description
Property Name	28	The name of the property that was modified. An event detail will be generated for each modified property.
Property Value	29	The new value for any modified property of the document or object. An event detail will be generated for each modified property.
Old Property Value	120	A user's old email address.
New Property Value	121	The same user's new email address.

Save

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed
  - "2" indicates the object was successfully saved or exported to a repository
  - "3" indicates the object was successfully saved or exported to a new format

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was saved or exported.
File Name	18	The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on

Event Detail	ID	Description
		open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable.

Search

A search was conducted.

- Event Type ID: 1009

Event Detail	ID	Description
Keyword	19	The keywords of the conducted search.
Category	20	Category used in the search (if applicable).
Number of Rows	63	The number of rows returned by the search.

Edit

User edited the content of an object.

- Event Type ID: 1010

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Query	25	If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.)
Universe Object Name	31	The name of the universe the document or object uses. A separate detail will be generated for each universe accessed by the document or object.
Container ID	32	The CUID of the container (a dashboard for example) that uses the object (if applicable).
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed

- "2" indicates the job failed but will be reattempted
- "3" indicates the job was cancelled

Event Detail	ID	Description
Size	17	Size of the document (in bytes) that was run.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Deliver

An object was delivered.

- Event Type ID: 1012

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable).
From address	41	Records the sender's address for documents/objects distributed by email (if applicable).
To address	42	Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient.
File Name	18	Records the file name of documents/objects distributed by email or FTP, or

Event Detail	ID	Description
		written directly to a disk that is not part of the Business Objects deployment.
Account Name	45	This records one of the following: • For *Inbox* delivered objects, a list of BusinessObjects user account names. • For *FTP* delivered objects, the FTP account name. • For *Unmanaged Disk* delivered objects, the login account used. • For *SMTP* delivered objects, the login account used for the SMTP server.
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	75	Indicates how the delivery was initiated: • "0" indicates scheduled • "1" indicates sent to a destination • "2" indicates published • "3" indicates an alert was triggered

Retrieve

An object is retrieved from the CMS.

- Event Type ID: 1013

Logon

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt

    - "2" indicates a named-user license logon was successful
    - "3" indicates a non-user (system) login was successful
- Event Type ID: 123
- Statuses:
    - "0" indicates a concurrent-user license logon was successful
    - "2" indicates a named-user license logon was successful

Event Detail	ID	Description
Concurrent User Count	50	The number of users on the system at the time the event was triggered.
Client hostname reported by client	51	Hostname of client as reported by client.
Client hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value is recorded.
Client IP address reported by client	53	IP address of client as reported by the client.
Client IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value is recorded.
Authentication Type	122	Authentication type is valid for the vlaues secEnterprise, secLDAP, secWinAD, secSAPR3
User Type	123	Type of the user.
Session Count	125	Count of the session is recorded.
Tenant ID	126	The ID of the tenant is recorded.
Concurrent Tenant Session	127	The count of the concurrent session of the tenant is recorded.

Logout

A user logs off.

- Event Type ID: 1015

Event Detail	ID	Description
Concurrent User Count	50	The number of concurrent users on the system at the time the event was triggered.

Trigger

A file event is triggered.

- Event Type ID: 1016

Event Detail	ID	Description
File Name	18	The name of the file that was being monitored and triggered the event.

23.3.1.1 Platform events

The following events are specific to the BI platform.

Rights Modification

Right or rights for an object were modified.

- Event Type ID: 10003

Event Detail	ID	Description
Rights Added	55	The type of right added, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`.
Rights Removed	56	The type of right removed, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
Rights Modified	57	The type of right modified, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
Principal	118	The ID of a user or user group (principal) for whom security rights were modified.
Principal Name	119	The name of a user or user group (principal) for whom security rights were modified.

Custom Access Level Modified

A Custom Access Level was modified.

- Event Type ID: 10004

Event Detail	ID	Description
Rights Added	55	The type of right added, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
Rights Removed	56	The type of right removed, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
Rights Modified	57	The type of right modified, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
Principal	118	The ID of a user or user group (principal) for whom security rights were modified.

Auditing Modification

A change was made to the system's auditing settings.

- Event Type ID: 10006

Event Detail	ID	Description
Event Type ID	58	Records the ID of the auditing event type that was enabled or disabled. If multiple event types are enabled or disabled in one action, an event detail will be generated for each event type.

Event Detail	ID	Description
Action	59	Records which auditing events were enabled or disabled.
New Auditing Level	60	If the auditing level of detail is changed, records the new level setting (off, minimal, or default for example).
Old Auditing Level	61	If the auditing level of detail is changed, records the previous level setting (off, minimal, or default for example).
Auditing option	62	If an optional detail is enabled or disabled, the detail modified is recorded and whether it was enabled or disabled. If multiple details are enabled or disabled in a single action, a detail record will be generated for each modified detail.
ADS Connection	78	If the connection to the Auditing Data Store is changed, this records the new connection settings using the following format: `DBType=Oracle,DBName=MyADS,Username=USR1,Password="*****",SSO=off,DBReconnect=on`. Only the details changed will be recorded. For example, if the user name is the only thing updated, then only `Username="new"` will be recorded. **Note** The password information will always be obscured with * in the database.
Auto Delete Interval	105	This detail will record any changes to the *Delete Events Older Than* field in the Auditing CMC page. This governs how many days auditing information will be maintained in the ADS.

23.3.1.2 Commentary Events

The following rights are specific to the **BI Commentary** in the Business Intelligence Platform.

Add Comment

This event is generated when you add a new comment, duplicate a comment, and when you add comments in bulk. When you add a comment, only the Parent Document ID is recorded. In case of duplication or bulk addition of comments, all the event details mentioned in the table below are recorded.

Event Type ID: 11001

Event Detail	ID	Description
Parent Document ID	12	Records ID of the object.
Description	24	Records any additional information in the event.
Size	17	Size of the object (in bytes) that is the subject of the event.
File Name	18	Records the file name of the object.

Get Comment

The event is generated when you view a comment.

Event Type ID: 11002

Event Detail	ID	Description
Parent Document ID	12	Records ID of the object.
Size	17	Size of the object (in bytes) that is the subject of the event.

Modify Comment

The event is generated when you edit an existing comment.

Event Type ID: 11003

Event Detail	ID	Description
Parent Document ID	12	Records ID of the object.

Delete Comment

The event is generated when you delete an existing comment.

Event Type ID: 11004

Event Detail	ID	Description
Parent Document ID	12	Records ID of the object.

Hide Comment

The event is generated when you hide a comment.

Event Type ID: 11005

Event Detail	ID	Description
Parent Document ID	12	Records ID of the object.

23.3.1.3 SAP BusinessObjects Web Intelligence events

The following events are specific to the SAP BusinessObjects Web Intelligence component.

Drill Out Of Scope

User drilled out of the report's scope.

- Event Type ID: 10201

Event Detail	ID	Description
Object Instance	11	Records if the event is the result of a scheduled update or a user viewing the object ("0" = resulted from a user viewing the object, "1" = resulted from a scheduled refresh of the object).
Number of Rows	63	The number of rows the database server returned.
Query	25	Records the query used to refresh the data (optional, set in CMC).

Event Detail	ID	Description
Universe Object Name	31	The name of the universe the document uses. An instance will be recorded for each universe accessed by the document.
Universe ID	32	The CUID of the universe the document uses. An instance will be recorded for each universe accessed by the document.

Page Retrieved

Web Intelligence document page was retrieved.

- Event Type ID: 10202

Event Detail	ID	Description
WebIntelligence report name	10220	Records the name of the WebIntelligence document report viewed.
Output Type	10221	The output format of the document viewed, e.g: • `xml.ro` for WebIntelligence • `pdf` for Adobe Acrobat • `xls` for Microsoft Excel • `text/xml` when unknown
Page Number	10222	Records the number of the WebIntelligence report page viewed. NB: • "0" when it cannot be retrieved (e.g. pdf) • "-1" in case of error

BW Statistics

> **Note**
>
> These audit events are directly sent to SAP BW. They are listed below for reference as Web Intelligence events, but aren't stored in the Auditing Data Store of the BI platform. They are available since 4.2 SP03.

Option	Possible Values	Description

Long name
`sap.sal.bics.postBWstatistics`
Short name
`postBWstatistics`
Default value: `false`
	`true`
	`false`
		Activates the following BW statistics events:
		• 20100: fetches BEx's characteristic members
		• 20101: fetches BEx query's results
		• 20102: submits BEx variables
		• 20103: opens a BEx query using BICS API.
		• 20104: synchronizes with BW
		• 20105: set variable's input string

23.3.1.4 SAP BusinessObjects Promotion Management console events

The following events are unique to the Promotion Management for SAP BusinessObjects component.

SAP BusinessObjects Promotion management tool common details

All Promotion Management events will have the following additional event details.

Event Detail	ID	Description
Element Cluster	6	The CUID of affected clusters when promotion management tool performs an operation on objects located in different clusters. An event detail will be generated for each affected cluster.
Element Comment	7	Additional information on the object.
Primary Element	8	If the element is a primary element, this detail will be set to "1"; if it is a dependent element, it will be set to "0".
Element Status	9	If the operation element fails this detail will be set to "1"; otherwise it will be "0".
Operation	10	Describes the type of operation performed (for example Add, Delete, or Modify).

SAP BusinessObjects Promotion management tool Configuration

Configuration of Promotion Management is changed.

- Event Type ID: 10900

Event Detail	ID	Description
Configuration	100	A user views the promotion management tool configuration. The configuration displays as comma-separated value pairs, for example: rollback settings=enabled, port=900.
Configuration Before	101	If the promotion management tool settings for an object are modified, records the previous configuration settings. Uses the same format as Configuration.
Configuration After	102	If the promotion management tool settings for an object are modified, records the new configuration settings. Uses the same format as Configuration.
VMS Type	10900	The type of version management system.

Rollback

An object was rolled back to a previous Version Management System (VMS) version.

- Event Type ID: 10901

VMS Add

A resource is added to the VMS.

- Event Type ID: 10902

Event Detail	ID	Description
Version	104	Records the version number of the document in the Version Management System.

VMS Retrieve

A resource is retrieved from the VMS.

- Event Type ID: 10903

Event Detail	ID	Description
Restore Deleted Object	103	Indicates if a retrieved object had been deleted from the system. "0" indicates the object was not deleted; "1" indicates the object was deleted.
Version	104	Records the version number of the document in the VMS.

VMS Checkin

A resource is checked into the VMS.

- Event Type ID: 10904

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.

VMS Checkout

A resource is checked out from the VMS.

- Event Type ID: 10905

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.

VMS Export

A resource is exported from the VMS.

- Event Type ID: 10906

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.

VMS Lock

A resource in the VMS is locked, to prevent users editing it.

- Event Type ID: 10907

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.
Locked By	10901	The user name of the user who performed the action.

VMS Unlock

A resource in the VMS is unlocked, allowing users to edit it.

- Event Type ID: 10908

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.
Unlocked By	10902	The user name of the user who performed the action.

VMS Delete

A resource is deleted from the VMS.

- Event Type ID: 10909

Event Detail	ID	Description
Version	104	Records the version number of the document in the Version Management System.

24 Events

24.1 About Events

Events are similar to flags or check points that provide information about events or actions that occur on the server. Event-based scheduling provides you with additional control for scheduling objects: you can set up events so that objects are processed only after a certain specified event occurs.

Here is a list of events that are available on the CMC:

Crystal Reports Events

Crystal Report events only trigger a report run if the report waiting on the event is already scheduled and ready to run. Crystal Reports events can be based on a new file and reports can be scheduled to wait for event triggering.

Custom Events

Custom events are also called "manual events". Every custom event has two properties: the event name and the corresponding description. Custom events are used to trigger alerts to a user's BI Inbox and the user's e-mail ID. Custom events also provide you with an option to schedule objects based on event triggering by setting the required conditions.

Monitoring Events

Monitoring events are system-generated events that relate to service health status. Monitoring is a built-in application in the CMC that allows administrators to monitor the health of the system. The most important aspects of monitoring are watches and probes.

Watches allow you to set thresholds for over 250 metrics within the system. You are notified when the set thresholds are breached.

> ✤ Example
>
> If you have a watch that monitors the disk space consumed by the Output FRS, you are notified when the consumption reaches the specified volume of disk space.

System Events

There are two types of system events:

- **File-based events**
  File-based events are based on any file located under a path. For example, if a file is located under one of the server paths, you can run reports by scheduling based on the path of a file. From a business perspective, if you consider the required tables for reporting get loaded on a monthly/weekly/daily basis, then placing a text file under a path after the reports have been loaded will trigger a file-based system event.
- **Scheduling-based events**
  Scheduling-based events are used to run reports or BI objects in a sequential manner. This event definition comprises three actions: success, failure and success or failure. This is because the status of a running object, at any given point in time, could either be success or failure.

User Notifications

User notification events are used by administrators to notify BI end users, who are using BI launch pad, about important events. Administrators can notify selected users about critical messages and other related information at the scheduled time (for example, system downtime). The alert message appears as a notification popup in the BI launch pad screen when the user logs on.

BW Events

In the BW system, the *BOE trigger event*, a process type in a BW process chain, triggers BW events for the BI platform. Each BW event comprises an event name and its description. BW events are used for configuring an event-based schedule of reports, which are based on a BW data source. A BW system triggers a BW event when data is changed in the system. BW events can also trigger alerts to a user's BI Inbox and e-mail ID.

24.1.1 User Notifications

Notification capability enables an Administrator to send alert messages from the CMC to the User. Using this feature, administrators can notify selected users about critical messages and other related information (for example, system downtime). The alert message appears as a notification popup on the top right corner in the BI launch pad screen when the user logs on.

24.1.1.1 Creating a Notification Event

Context

The notification event is a schedulable plug-in. When creating a new notification event, the administrator is required to specify the 'Start' and 'End' date and time. The adaptive job server that is responsible for scheduling creates a scheduling instance when the specified 'Start' time of the notification is met. The AJS then pushes the alert to the alerts inbox in the launch pad. These notifications appear on the top right corner in the BI launch pad screen.

To create a notification event, proceed as follows:

Procedure

1. Log on to the CMC.
2. In the CMC Homepage, select *Events* from the dropdown menu.
3. From the *Events* pane on the left, right-click on *User Notifications* and navigate to *New* > *New Notification*.

   The *New Notification* popup window appears.
4. To schedule a notification message, proceed as follows:
   a. Select the required time zone from the *Time Zone* dropdown menu.
   b. Set the required *Start Date/Time*.
   c. Set the required *End Date/Time*.

   > **Note**
   >
   > - The *End* time cannot be earlier than the *Start* time.
   > - The difference between the *Start* and *End* time cannot exceed 14 days.
   > - Regardless of the time zone selected, the *Start* time cannot be earlier than the CMS server time. If the *Start* time is earlier than the CMS server time, the notification will not be triggered.

   d. In the *Notification Title* box, enter the title of the notification.

   > **Note**
   >
   > The *Notification Title* cannot exceed 256 characters in length.

   e. In the *Description* box, enter an appropriate description for the notification.

   > **Note**
   >
   > The *Description* cannot exceed 1024 characters in length.

> **Note**
>
> You can choose to send the notification to the user's e-mail by selecting the *Send this message as notification to user's e-mail ID* checkbox.

5. Choose *OK*.

Results

You have now successfully created a notification event.

> **Note**
>
> In the Notification Properties page, the created and modified time reflect the CMS server time.
>
> The administrator can disable the auto-popup of the notification banner in the BI Launch pad by modifying the `BIlaunchpad.properties` file and disabling the polling by setting `Notification.enabled` field to `false`. In order for notification polling to work by default, the `pinger.enabled` property in `global.properties` file must be enabled. If polling and pinger are not enabled, the notification popup only appears when a user refreshes the page, logs in for the first time, or logs in again when the notification is active.
>
> Polling happens once every 3 minutes in the BI launch pad.

24.1.1.2 Selecting a Notification Audience

Notification capability allows you to select the required audience for every notification you create.

Context

To select the audience for a notification, proceed as follows:

Procedure

1. Right-click the notification you created and select *Manage Subscribers* from the context menu.

   The *Manage Subscribers* popup window appears.
2. From the *Subscriber List* pane, choose *Add*.

   The *Add Subscribers* popup window appears.
3. Select the required user/user groups whom you want to notify.

4. Choose *Add Default Subscription(s)*.

   The *Add Subscribers* popup window disappears.
5. From the *Manage Subscribers* popup window, choose *Save and Close*.

Results

You have now successfully selected the audience for a notification.

> **Note**
>
> - You cannot modify the subscription list after the notification is triggered.
> - You can now send notifications to the OpenDocument users.

24.1.1.3 Editing a Notification Event

Context

To edit a notification event, proceed as follows:

Procedure

1. Log on to the CMC.
2. In the CMC Homepage, select *Events* from the dropdown menu.
3. From the *Events* pane on the left, choose *User Notifications*.
4. Right-click on the notification you want to edit and select *Edit Event* from the context menu.

   The *Edit Event* dialog box appears.
5. Edit the required parameters of the notification event.

   > **Note**
   >
   > You can edit the following parameters of a notification event:
   > - Time Zone
   > - Start Date/Time
   > - End Date/Time
   > - Notification Title
   > - Description

- Manage Subscribers

6. Choose *OK*.

Results

You have now successfully edited a notification event.

> **Note**
>
> If you edit a notification event by navigating to *Events* > *User Notifications* > *Properties*, the notification will not be triggered unless you choose *OK* on the *Edit Event* page.

25 Platform Search

25.1 Understanding Platform Search

Platform Search enables you to search content within the BI platform repository. It refines the search results by grouping them into categories and ranking them in order of their relevance.

In this version of the BI platform, Platform Search has the following features:

- Search for BI platform content.
- Suggest a query for creating a document if it cannot find an existing document.
- Support both continuous and schedule-based indexing.
- Support indexing in a clustered environment.
- Set and modify the level of indexing.
- Provide advanced search configuration options.
- Support multilingual search and indexing.
- Provide an advanced search syntax.
- Support metadata, content, and dynamic facets.
- Support self healing based on the system load.

> **Note**
>
> If you migrate from the previous version to a new version, the index is not migrated.

25.1.1 Platform Search SDK

Platform Search supports a public SDK that functions as an interface between the client application and Platform Search. It is publicly exposed to help you customize the search service and integrate it with your application.

When a search request parameter is sent through the client application to the SDK layer, the SDK layer converts the request parameter into XML-encoded format and passes it to the Platform Search Service.

For more information about the Platform Search API, see the *Business Intelligence platform Java API Reference*.

25.1.2 Clustered Environment

Platform Search can share the load across multiple nodes in a clustered environment. The deployment in a clustered environment optimizes system resources and enhances server performance.

Platform Search supports both horizontal and vertical clustering for both search and indexing features. With clustered environments, it optimizes the performance of both search and index processes.

For more information on how to configure Platform Search Index location in a clustered environment, please check this SAP Note.

Load balancing

Platform Search supports load balancing for both indexing and searching. In a clustered environment, indexing and search requests can be executed on multiple nodes to share the load. Each node functions independently to index the content and create delta indexes. However, only one node in the cluster will act as a master index and merge the delta indexes into the master index. All nodes can access the master index. This enables simultaneous search requests.

Failover

The failover mechanism ensures that users can continue to search and use the index operation without disruption. When a node in the cluster becomes unavailable due to a technical failure or maintenance-related activities, another node automatically takes over the process of indexing and searching requests.

25.2 Setting Up Platform Search

25.2.1 Deploying OpenSearch

Platform Search supports the OpenSearch standard, enabling client applications to use the OpenSearch standard or format to communicate with Platform Search. OpenSearch is not installed by default with the SAP BusinessObjects Business Intelligence suite, so users need to deploy it manually as a separate WAR file (`opensearch.war`) to an application server such as Tomcat, or using the WDeploy tool. This file is copied into the `<INSTALLDIR>\warfiles\OpenSearch` directory by the installer.

> **Note**
>
> Client programs need to follow the OpenSearch standards to communicate with Platform Search.

> **Note**
>
> When you install the BI platform, the Tomcat application server is installed by default.

25.2.1.1 Deploying Manually

Context

To deploy OpenSearch in a BI platform environment, perform the following steps:

Procedure

1. Go to the following location: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Copy the OpenSearch folder into `<INSTALLDIR>\tomcat\webapps\`.
3. Change the configuration parameters in the `\OpenSearch\WEB-INF\config.properties` file:
   - CMS: the CMS name with port number: `<CMS Name>:<Port Number>`.
   - OpenDocURL: the URL of the OpenDocument application: `http://<tomcathost>:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   - Proxy.rpurl: the reverse proxy server name is required if you want to use reverse proxy.
   - Proxy.opendoc.rpurl: the opendoc reverse proxy server name is required if you want to use the reverse proxy.
4. Restart the Tomcat application server to deploy OpenSearch.

25.2.1.2 Deploying using WDeploy

Context

For Windows, commands are described as `wdeploy.bat <parameters>`. For UNIX, commands are described as `wdeploy.sh <parameters>`.

Procedure

1. Update the `config.<ApplicationServer>` file located at `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` with the required web application server parameters (for example, installation directory, instance name, administrator port, administrator user name, and administrator password).
2. Change the following parameters in the `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties` file:

a. For the `CMS` parameter, enter `<CMSName>:<Port>`.
b. For the `OpenDocURL` parameter, enter the URL of the OpenDocument application.

   The URL should be `http://<WebApplicationServerHost>:<ConnectorPort>/BOE/OpenDocument/opendoc/openDocument.jsp`.
c. (Required for reverse proxy) For the `Proxy.rpurl` parameter, enter the reverse proxy server name.
d. (Required for reverse proxy) For the `Proxy.opendoc.rpurl` parameter, enter the OpenDocument application's reverse proxy server name.

3. Execute the `wdeploy.bat <WebApplicationServer> -Dapp_source_tree=<ParentFolderOpenSearchWebApp> -DAPP=OpenSearch deploy` command from `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   For example, the following command deploys OpenSearch to a WebSphere 7 web application server:

```
wdeploy.bat websphere7 -Dapp_source_tree="<InstallDir>\SAP BusinessObjects
Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```

4. Restart the web application server.

25.2.2 Configuring reverse proxy

Context

To deploy web applications on a Web application server located behind the reverse proxy server, configure a reverse proxy server to map incoming URL requests to the correct WAR file.

To illustrate the configuration steps, we use Apache 2.2 Reverse Proxy server as an example. To configure Apache 2.2 Reverse Proxy server for OpenSearch:

Procedure

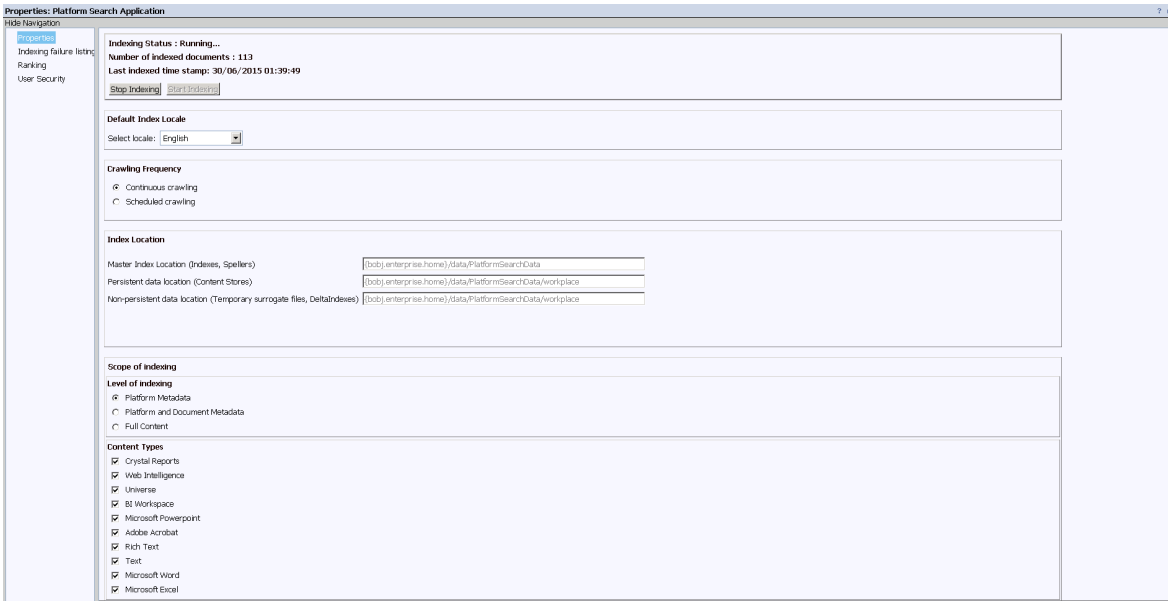
1. Set up the reverse proxy and make the changes in the `WEB-INF\config.properties` file of OpenSearch.
2. Enable the following context parameters and change the values accordingly.
   - `proxy.rpurl`: This is the reverse proxy URL for OpenSearch (such as `http://machineIPAddress/RP/OpenSearch/`).
   - `proxy.opendoc.rpurl`: This is the reverse proxy URL for Open Doc (such as `http://machineIPAddress/RP/BOE/`).
3. Update the `httpd.conf` file, located under the Apache Reverse Proxy installation folder, with the following settings:
   - `ProxyPass /RP/BOE/OpenDocument/ http://<Tomcat host>:<Connector Port>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<Tomcat host>:<Connector Port>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`

4. Restart the Apache 2.2 Reverse Proxy server.

25.2.3 Configuring Application Properties in the CMC

To configure the Platform Search application properties, complete the following steps:

1. Go to the *Applications* area of the CMC.
2. Select *Platform Search Application*.
3. Click *Manage* > *Properties*. The *Platform Search Application Properties* dialog box appears.



4. Configure the Platform Search settings:

Option	Description
Search Statistics	Platform Search offers the following search statistics: • Indexing Status: displays the status of the indexing process. • Number of indexed documents: displays the number of documents that are indexed. • Last indexed time stamp: displays the time stamp at which the document was last indexed.
Stop / Start Indexing	Start or Stop Indexing options enable you to start or stop the indexing process when you want to switch from continuous crawling to scheduled crawling, or for maintenance purposes. To stop indexing, click *Stop Indexing*.

Option	Description
Default Index Locale	Platform Search uses the locale specified in the CMC for indexing all the non-localized BI documents. Once the document is localized the corresponding language analyzer is used for indexing. Search is based on the client's product locale, and the weighting is given to the client's product locale. You can configure the weighting in the CMC configuration properties.
Crawling Frequency	You can index the entire BI platform repository by using the following options: • Continuous crawling: With this option, indexing is continuous; the repository is indexed whenever an object is added, modified, or deleted. It allows you to view or work with the most up-to-date BI platform content. Set by default, continuous crawling updates the repository continuously with the actions that you perform. Continuous crawling works without user intervention, and reduces the time taken for indexing a document. • Scheduled crawling: With this option, indexing is based on the schedule set by the Schedule options. For more information about scheduling an object, refer to the *Scheduling an Object* section of Platform Search in the *SAP BusinessObjects Business Intelligence platform CMC Online Help*. **Note** • If you select *Scheduled Crawling* and set the *Recurrence* to an option other than *Now*, Platform Search displays the date and time stamp when the document is scheduled to be indexed next. • If you select *Scheduled Crawling*, then the *Start Indexing* button is enabled and the *Stop Indexing* button is disabled. • Once the scheduling is complete, the *Stop Indexing* button is disabled.

Option	Description
Index Location	The indexes are stored in shared folders in the following locations: • Master index location (indexes and speller): The master and speller indexes are stored in this location. During a search, the initial results are retrieved using the Master Index, and the speller indexes are used to retrieve suggestions. In a clustered BI platform deployment, this location should be on a shared file system that is accessible from all nodes in the cluster. • Persistent data location (Content stores): The content store is placed in this location. It is created from the master index location and remains synchronized with it. The content store is used to generate facets and process the initial hits generated from the Master Index location. In a clustered BI platform deployment, content stores are generated at every node. The persistent data location is the only index location that is affected by the clustered environment as it contains the content store folders. If a machine has a single search service, then there will be only one content store location. For example, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. However, in a clustered environment, if there are multiple search services, then each search service will have one content store location. For example, if you have two instances of a server running, then the content store locations would be as follows: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name 1>\ContentStores. • Non-persistent data location (Temporary files, Delta Indexes): In this location, the delta indexes are created and stored temporarily before being merged with the Master index. The indexes at this location are deleted once they are merged with the Master Index. In addition, surrogate files (output of the extractors) are created in this location and stored temporarily until they are converted into delta indexes. **Note** • Master index location must be a shared location. • You need to click *Stop Indexing* to modify the index location. • If you modify an index location, copy the content to a new location, or the existing index information will be lost. • The index files might store personal and confidential information, especially when you choose to index document content. You must allow only a system user to access the shared folder and you should store the shared folders in an encrypted environment to avoid data theft.

Option	Description

Level of indexing	You can tune the search content by setting the level of indexing in the following ways:
	• Platform Metadata: An index is created only for the platform metadata information such as titles, keywords, and descriptions of the documents. By default, this option is selected.
	• Platform and Document Metadata: This index includes the platform metadata as well as the document metadata. The document metadata includes the creation date, modification date, and name of the author.
	• Full Content: This index includes the platform metadata, document metadata, and other content such as:
	  • The actual content in the document
	  • The content of prompts and LOVs
	  • Charts, graphs, and labels
	Note
	Full content indexing is not supported for Analysis Office and Lumira documents. Only metadata indexing is supported for Analysis Office and Lumira documents.
	Note
	When you modify the level of indexing, the indexing is initialized for the entire BI platform repository refresh.

Content Types	You can select the following content types for indexing: • Crystal Reports • Web Intelligence • Universe • BI Workspace • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Rich Text • Text • Microsoft Word • Microsoft Excel The content type filter does not apply for platform metadata indexing. Regardless of the content types you select, platform metadata indexing happens for all the supported object types and the search results in BI launch pad returns all the objects for the keyword related to platform metadata. The content type filter is relevant for document metadata indexing (document author, document header, document footer, and so on) and content indexing (graphs , charts , table with a report). Based on the level of indexing and content types you select, platform search indexes the document metadata and content for the selected objects types from the repository and only those objects appear in the BI launch pad search results, when searching for keyword related to document metadata and content.

Option	Description
Rebuild index	This option deletes the existing index and re-indexes the entire repository. You can select the *Rebuild index* option whether indexing is running or stopped. The existing index is deleted when you save your changes to the properties page. However, if indexing is currently stopped, the index does not start rebuilding until you restart indexing. If you do not want Platform Search to re-index the documents, clear the *Rebuild index* option before clicking *Start Indexing*.
Documents Excluded from Indexing	The *Documents Excluded from Indexing* option excludes documents from indexing. For example, you may not want extremely large Crystal reports to be made searchable to ensure the report application server resources are not overloaded. Similarly, you may not want publications with hundreds of personalized reports to be indexed. By excluding particular documents, you can prevent them from being accessed by Platform Search. It is important to note that if a document is already indexed before it is put into this group, the document may still be searchable. To ensure that documents in the *Documents Excluded from Indexing* group are not searchable, you must rebuild the index. By default, only the Administrator account has full control of the *Documents Excluded from Indexing* option. Other users with the following rights can only add documents to the *Documents Excluded from Indexing* group: • View and edit rights on the category • Edit the document directly
Other Configuration - Skip Instance	By default, instances of documents are picked for indexing. This causes inflated index size resulting in more consumption of disk space. The size of "Lucene Index Engine" folder within PlatformSearchData folder grows huge due to indexing of huge number of instances in the repository. If there are millions of documents (or more) and many of these documents also have huge number of existing instances (along with scheduled instances generated in regular interval) in the system, then the size of "Lucene Index Engine" folder grows excessively even if the indexing level is set to "Platform Metadata". Platform Search Skip Instance feature allows you to control the indexing of instances by enabling or disabling, through check box under 'Other Configuration - Skip Instance' in Platform Search Application properties page in CMC. **Note** • If you Enable/Disable Skip Instance, you need to restart Platform Search Adaptive Processing Server. This change affects all levels of indexing. • If you modify Skip Instance and want the changes to be applied to all existing instances (i.e. to be picked for indexing), then you need to rebuild index.

Option	Description
Objects Excluded from Indexing	The *Objects Excluded from Indexing* option excludes objects from indexing. For example, you may not want certain objects to be made searchable to ensure the report application server resources are not overloaded. By excluding particular objects, you can prevent them from being accessed by Platform Search. It is important to note that if an object is already indexed before it is put into this group, the object may still be searchable. To ensure that documents in the *Objects Excluded from Indexing* group are not searchable, you must rebuild the index. List of objects that can be excluded from indexing: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • Rtf • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • Profile • Event • Discussions • InformationDesigner • MDAnalysis • Publication • Agnostic • Analytic • Hyperlink • Program • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset • VISI.Lums

Option	Description
	• VISILums • User • UserGroup

5. Click *Save & Close*.

> **Note**
>
> If a user does not select the *Rebuild Index* option and changes the level of indexing or selects or deselects extractors, then the index is incrementally updated without deleting the existing index.

25.3 Working with Platform Search

25.3.1 Indexing Content in the CMS Repository

Indexing is a continuous process that involves the following sequential tasks:

1. Crawling: Crawling is a mechanism that polls the CMS repository and identifies objects that are published, modified, or deleted. It can be done in two ways: continuous and scheduled crawling.
   For more information on continuous and scheduled crawling, refer to the *Configuring Application Properties* topic in Related Topics.
2. Extracting: Extracting is a mechanism to call the extractors based upon the document type. There is a dedicated extractor for every document type that is available in the repository. New document types can be made searchable by defining new extractor plug-ins. Each of these extractors is scalable enough to extract content from large documents that contain many records.
   The following extractors are supported:
   - Metadata extractor
   - Crystal report extractor
   - Web Intelligence extractor
   - Universe extractor
   - Agnostic extractors (MS Office 2003 and 2007 and PDF documents)

   For more information on searchable document types, refer to the *Searchable content types* topic in Related Topics.
3. Indexing: Indexing is a mechanism that indexes all the extracted content through a third-party library, called Apache Lucene Engine. The time required for indexing varies, depending on the number of objects in the system, and the size and type of documents.
   For indexing to run successfully, the following servers must be running and enabled:
   - Input File Repository Server (IFRS)
   - Output File Repository Server (OFRS)
   - Central Management Server (CMS)
   - The Adaptive Processing Server (APS) that hosts the Platform Search service

If the object type is selected as Web Intelligence or Crystal report, the corresponding Web Intelligence Processing Server or Crystal Reports Application Server must be running and enabled for the respective object types selected.

4. Content Store: The content store contains information such as id, cuid, name, kind, and instance extracted from the main index in a format that can be read easily. This helps to quicken the search process.

Related Information

Configuring Application Properties in the CMC [page 865]
Searchable Content Types [page 873]

25.3.2 Indexing Failure Listing

Context

The indexing failure listing provides a list of documents that fail to get indexed. platform Search offers three attempts for a document to get indexed. If a document fails to get indexed, it is listed in the indexing failure listing.

To view the indexing failure listing, complete the follwoing steps:

Procedure

1. Go to the "Applications" area of the CMC.
2. Select *Platform Search Application*.
3. Choose*Actions > Indexing failure listing*.

   The "Platform Search Application" dialog box appears, displaying a list of documents with the following details:
   - Title: Displays the title of the document that failed to get indexed.
   - Type: Displays the name of the document type, such as Crystal Report and Web Intelligence, and the location of the document.
   - Failure Type: Displays the error code and the reason for index failure of the document. Click the More info hyperlink to learn more about the stack trace of the cause of the error.
   - Last attempted time: Displays the time stamp of the last attempt to index a document.

25.3.3 Searching Results

25.3.3.1 Pre- Search

25.3.3.1.1 Suggested Queries

When using Platform Search, a user may be trying to find answers to a specific question rather than looking for a specific object. These questions may or may not be answered in reports available in the BI platform repository.

Platform Search analyzes the structure of universes and existing reports in your repository and compares this information to the search request that the user has provided to suggest new SAP BusinessObjects Web Intelligence queries that may help users find the answers to their questions.

To create potential reports, Platform Search matches the words in all universes for dimension, measure, condition and filter value.

Platform Search looks for matches in the following information about universes or existing Web Intelligence documents:

- Measures in universes that match words in the search input.
  When a measure matches one of the search terms, that measure will be used in the resulting Web Intelligence document.
- Dimension names in universes that match words in the search input.
  When a dimension name matches one of the search terms, the resulting Web Intelligence document breaks down the information on this dimension.
- Query filters may be used to focus the data shown in the document. These query filters are generated by analyzing the search input.
  - If the name of a universe condition matches one of the search terms, the condition is used as the filter.
  - If there are field values in existing Web Intelligence documents whose names match search terms, a filter will be created from the dimension from the historical report with the matched value, using "equal to" as the condition operator.

If Platform Search has made enough matches that the resulting document will contain two result fields and one filter, the query is considered to be ready to run. In this case, the user can click to view the completed report.

If there are insufficient number of matches between universes and the document, you can edit the query before running it.

Platform Search suggests multiple queries if several universes matches the search input, or if the same word appears in two different matches, such as in the name of a dimension and as a filter value.

25.3.3.1.2 Searchable Content Types

The content published to the BI platform is searchable with Platform Search. The object types are listed below with their corresponding indexed content:

Object Type	Indexed Content
Crystal Reports 2025	Title, description, selection formula, saved data, text fields in any section, parameter values, and sub-reports.
Web Intelligence documents	Title, description, name of the universe filters used in the report, saved data, constants in the filter condition locally defined in the report, name of the universe measures used in the report, name of the universe objects used in the report, data in record set, and static text in cells.
Microsoft Excel documents (2003 and 2007)	Data in all non-empty cells, fields on the Summary page of the document properties (title, subject, author, company, category, keywords and comments), and text in document headers and footers. For cells that use calculation or formula, the value after the evaluation is searchable. For number or date/time values, the raw data is searchable.
Microsoft Word documents (2003 and 2007)	Text in all paragraphs and tables, fields on the Summary page of the document properties (title, subject, author, company, category, keywords and comments), text in document headers and footers, and numerical text.
RTF, PDF, PPT and TXT Files	All text in these files is searchable.
LCMJob, ObjectPackage, Web service query (QaaWS), Profile, Discussions, InformationDesigner, widgets for SAP BusinessObjects BI platform, MDAnalysis, Publications, Analytic, and Hyperlink	Metadata content is searchable.
Events	All events such as Custom events, System events, Crystal Reports events and Monitoring events are searchable. If an event is associated with a source, Platform Search surfaces the source along with the event. **Note** Platform Search supports events for Crystal Reports for Enterprise.

Object Type	Indexed Content

BI Workspace	• The title, description, and contents of the following BIW modules are indexed:
	  • Text module
	  • Web Page module
	  • Navigation List module
	  • Viewer module
	• The title and description of a Compound Module is indexed.
	• Only the title of a Workspace Template Module is indexed.
	• In the case of a Group module, the title and metadata of the modules within it, is indexed.
	• The title, description, and CUID of InfoObject modules in BIW are indexed.
	  Note
	  Since only the title and description of an embedded InfoObject module is indexed, attempts to search for the InfoObject content, will not return references to the embedded module. For example, if a CR is inserted in BIW, its title and description is indexed. Any attempts to search for the contents of the CR will not return references to the embedded module.
	• If a BIW contains multiple tabs and sub-tabs, the title and contents of each tab and sub-tab, is also indexed.

Object Type	Indexed Content
Universe	Data content is searchable. **Note** By default, the universe indexing option is enabled. If you notice that queries used by Platform Search to index universe content take a long time to run, and impact database server performance, then we recommend disabling the universe indexing option in the Central Management Console (CMC). An example of a query that Platform Search uses while indexing universe content is `Select distinct SampleColumnName from SampleTableName LIMIT 1000`. Follow these steps to disable universe indexing: 1. Logon to the Central Management Console (CMC). 2. Choose *Applications*. 3. Navigate to Platform Search Applications and choose *Properties*. 4. Navigate to content types and uncheck *Universe*. 5. Choose *Save & Close*.
Lumira document	Only metadata content is searchable.
Analysis Office document	Only metadata content is searchable.

Note

The maximum size supported for Agnostic documents (MS Office 2003 and 2007 and PDF documents) is 15 MB.

25.3.3.2 Search

When a user searches for a keyword from BI launch pad or any other application that uses the Platform Search SDK, the master index is checked for their search terms. Based on the user's view rights, the search engine displays only those documents for which a user has the access rights.

Note

When search is done in the CMC in an environment with a large CMS DB, the search may fail. For more information, please check SAP Note 2156647 Searching in the CMC is slow or does not bring back results.

25.3.3.3 Post- Search

25.3.3.3.1 Facets

Platform Search refines the search results by grouping them into categories or facets of similar object types, and ranking them in order of the number of occurrences of the category among the returned results for the search term. Facets enable you to navigate to the exact result.

Platform Search generates facets from InfoObject metadata, document metadata, and document content. It displays only those facets that have more than two documents matching a specified query. Facets are surfaced dynamically based on the documents that match the search query and are sorted by document count.

Documents are grouped into the following generic facets or categories:

- Personal or public (such as HR, Corporate, and Finance): This is based on the BI platform document categories.
- Document type: This is based on the document type such as Web Intelligence, Crystal Reports, Microsoft Word (2003 and 2007) and Microsoft Excel (2003 and 2007).
- Universe and Connections: This is based on the content source.
- Date: This includes the last refreshed date: (year, quarter and month).
- Time: This includes the last refreshed time, such as, 24 hours and last week.
- Author: This is the name of the user who created the document.

> **Note**
>
> When working in Hebrew or Arabic locale, if you search for content objects in BI launch pad, the search result does not display facets.

25.3.3.3.2 Normalizing the Search Results Ranking

Platform search considers the place of occurrence of the searched term when ranking a document. It groups the content into the following categories based on the occurrence of the content in the document:

1. Platform Metadata
2. Document Metadata
3. Content Metadata
4. Content

You can configure the weighting for these categories in the CMC.

25.3.3.3.2.1 Customizing Weight for Ranking Search Results

Context

Platform Search allows you to set weights for the content grouped in categories based on the occurrence of the content in the document, so that you can set a higher value for the desired category to retrieve related search results faster.

To set the weight, perform the following steps:

Procedure

1. In the *Manage* area of the CMC, click *Applications*.
2. Open *Platform Search Application*.
3. Choose *Ranking*.

   The weights of different content categories such as Platform Metadata, Document Metadata, Content Metadata and Content are shown. The *User locale* is the locale set in the BI launch pad Preferences.
4. Set the weights to meet your requirements.
5. Choose *Save*.

Results

In an upgrade scenario, if ranking needs to be applied for documents that are already indexed, you need to rebuild the index. For more information, refer to information about rebuilding the index in the Configuring Application Properties in the CMC [page 865] section.

25.3.3.3.3 Multilingual Support

Platform Search offers multilingual support to index content, retrieve search results and get suggestions in your desired language. To index all non-localized BI platform documents, it uses the locale set in the *Default Index Locale* in the CMC.

Once the InfoObject is localized, Platform Search uses the corresponding language analyzer to index the document.

Search is based on the locale set as the Client's Product Locale. Platform Search gives more weighting to the Client Product locale while retrieving search results. You can configure the weights in the CMC.

25.3.3.3.4 Suggestions

Platform Search offers suggestions for incorrectly-spelled search queries. If the original search query does not yield any results, then Platform Search suggests the most probable terms based on the indexed content.

Suggestions appear as keywords with a hyperlink. Click a hyperlink to view a list of documents containing the keyword that may match your original query. These suggestions are determined algorithmically based on various objective factors.

If there are multiple terms that may match the original request, Platform Search suggests the top three suggestions in the language set as the *Default Index locale* in the CMC.

> **Note**
>
> Platform Search does not generate suggestions in these cases:
>
> - If the search queries contain fewer than three letters
> - For attributed searches, such as Type: Crystal Report
> - For universe metadata and content
> - For multi-byte languages such as Chinese, Japanese, and Korean

25.4 Auditing

All the events of search requests sent from a client application that uses the Platform Search Service and the search response are audited. For Platform Search, the auditing is implemented at the service level.

The Platform Search Service must run with a Client Auditing Proxy Service on the same server in order to send audit events.

There is one Event Type ID 1009 for Platform Search and four Platform Search-specific Event Detail Type IDs:

- Keyword searched (ID: 19)
- Number of Search Results (ID: 63)
- Facet Search (ID: 20)
- Search Exception (ID: 1)

Apart from the above event details, there are a few standard event details like sessionCuid and userCuid which are supported for any auditing in any BI platform module.

How auditing works in Platform Search is explained below with an example.

If you search a keyword such as "Sales", the total number of search results could be 5. In this case, the following events are audited:

- Event Type ID 1009
- Event Detail Type ID 19 with the value sales
- Event Detail Type ID 63 with the value 5
- Session CUID
- User CUID

- Status with value 0 which is success state
- Start time
- Duration
- Object ID with value 0 since this is service-side auditing

When Facets are generated and you select one or more facets, the following events are audited:

- Event Type ID 1009
- Event Detail Type ID 19 with the value sales
- Event Detail Type ID 63 with the value 5
- Event Detail Type ID 20 with comma separated string of facets
- Session Cuid
- User Cuid
- Status with value 0 which is success state
- Start time
- Duration
- Object ID with value 0 since this is service side auditing

If there is a search exception due to an invalid entry (for example *"a"), the following event details are audited:

- Event Type ID 1009
- Event Detail Type ID 19 with the value sales
- Event Detail Type ID 63 with the value 0
- Event Detail Type ID 1 with the exception message
- Session Cuid
- User Cuid
- Status with value 1 which is failure state
- Start time
- Duration
- Object ID with value 0 since this is service side auditing

25.5 Troubleshooting

25.5.1 Self Healing

Platform Search has its own self-healing mechanism. It continuously monitors the search service memory usage and stops indexing automatically when memory usage exceeds the threshold value. It automatically starts after the memory usage reduces to a reasonable limit. However, users can continue to search during this process but cannot index for a specific period of time. By default, Platform Search configures the number of documents that can be indexed at any instant, based on the document type. The indexing is initiated based on the system resources like CPU and memory.

25.5.2 Problem Scenarios

This section provides step-by-step solutions to a wide range of problems that may occur while retrieving search results with Platform Search.

Unable to retrieve search results from the newly added document containing the keyword

- Check if Platform Search supports the document type of the submitted document. If the document type is not supported, then the document is not indexed.
  For more information about supported document types, refer to the topic *Searchable Content Types* in the Related Topics listed below.
- Check the option selected for *Crawling Frequency*. If the *Crawling Frequency* is set to *Continuous crawling*, documents are picked immediately for indexing. If the *Crawling Frequency* is set to *Scheduled crawling*, indexing is executed only during the scheduled time period.
  For more information about *Crawling Frequency*, refer to the topic *Configuring Application Properties* in the Related Topics listed below.
- Check the Indexing failure listing to verify if the document is indexed successfully. If the document is displayed in this list, then you need to modify and re-submit it so that Platform Search uses the document for indexing.

  > **Note**
  >
  > You can modify the document by adding or deleting a field and then saving it again. This updates the document's timestamp in the BI platform repository and initiates the re-indexing of the document.

  For more information about documents that fail to be indexed, refer to the topic *Indexing failure listing* in the Related Topics listed below.
- Check the Adaptive Processing Server trace logs containing information about the indexing failure.
  1. Go to the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\` directory, containing the APS trace log with a .glf extension.
  2. Open the trace log file and search for the document SI_ID, that needs to be indexed.

     > **Note**
     >
     > You can find the document SI_ID from the document properties.

Unable to retrieve Crystal Reports documents

Platform Search indexes Crystal Reports content only for Crystal Reports 2025.

If the document contains indexable content, then you need to follow the same process as listed in the above mentioned section *Unable to retrieve search results from the newly added document containing the keyword*.

Related Information

Indexing Failure Listing [page 872]
Configuring Application Properties in the CMC [page 865]
Searchable Content Types [page 873]

26 Federation

26.1 Federation

Federation is a cross-site replication tool for working with multiple BI platform deployments in a global environment.

Content can be created and managed from one BI platform deployment and replicated to other BI platform deployments across geographical sites on a recurring schedule. You can complete both one-way replication and two-way replication jobs.

The benefits of Federation include the ability to:

- Reduce network traffic
- Create and manage content from a single site
- Increase performance for end users

When you replicate content using Federation, you can:

- Simplify administration needs for multiple deployments
- Provide a consistent rights policy across multiple offices for global organizations
- Obtain information faster and process reports at remote sites where data resides
- Save time by retrieving local and dispersed data faster
- Synchronize content from multiple deployments without writing custom code

Federation allows you to have separate security models, lifecycles, testing, and deployment times, as well as different business owners and administrators. For example, you can delegate administration features that restrict the sales application administrator from changing a human resources application.

You can replicate a variety of objects with Federation, as described in the following table.

Category	Object types you can replicate	Additional notes
Business Views	Business View Manager, DataConnection, LOVs, Data Foundation, and so on	All objects are supported, although not at the individual level.
Reports	Crystal reports, Web Intelligence, and Dashboard Design	Full client add-in and templates are supported.
Third-Party Objects	Excel, PDF, PowerPoint, Word, text, rich text, and Shockwave files	
Users	users, groups, Inboxes, Favorites, and Personal Category	
Business Intelligence Platform	Folders, Events, Categories, Calendars, Access Levels, Hyperlinks, Shortcuts, Programs, Profiles, Object Packages, Agnostic	

Category	Object types you can replicate	Additional notes
Universe	Universe, Connections, and Universe Overload	

The following scenarios highlight two examples of how your organization can use Federation.

Scenario 1: Retail (centralized design)

ACME store wants to send a monthly sales report to the different store locations using the one-way replication method. The administrator at the origin site creates a report that administrators at each destination site replicate and run against that store's database.

> → Tip
>
> Localized instances can be sent back to the origin site that maintain each object's replicated info. For example, it will apply the appropriate logo, database connection information, and so on.

Scenario 2: Remote Schedule (distributed access)

The data is at the origin site. Pending replication jobs are sent to the origin site to run. Completed replication jobs are then sent back to the destination sites for viewing. For example, the data for a report may not be available on the destination site, but the user can configure the reports to run on the origin site before the completed report is sent back to the destination site.

26.2 Federation terms

The following list of terms introduces words and phrases that relate to Federation and may assist with its navigation and use.

BI application	The logical grouping of related Business Intelligence (BI) content with a specific purpose and audience. A BI application is not an object. One BI platform deployment can host multiple BI applications, each of which can have a separate security model, lifecycle, testing and deployment timeline, as well as separate business owners and administrators.
Destination site	A BI platform system that pulls replicated BI platform content from an origin site.
Local	The local system where a user or administrator is connected. For example, the administrator of a destination site is considered “local” to the destination site.
Locally run completed instances	Instances that are processed on the destination site and then sent back to the origin site.
Multiple origin sites	More than one site can serve as an origin site. For example, multiple development centers generally have multiple origin sites. However, there can be only one origin site per replication.
One-way replication	Objects are replicated only in one direction: from the origin site to the destination site. Any updates made at a destination site remain at that destination site.
Origin site	The BI platform system where the content originates.

Remote	A system that is not local to a user. For example, the origin site is considered “remote” to users and administrators of the destination site.
Remote connection	An object that contains information used to connect to a BI platform deployment, including username and password, CMS name, WebService URI and clean-up options.
Remote scheduling	Schedule requests that are sent from the destination site to the origin site. Reports on destination sites can be scheduled remotely, which sends the report instance back to the origin site for processing. Then the completed instance is returned to the destination site.
Replication	The process of copying content from one BI platform system to another.
Replication job	An object that contains information about replication scheduling, which content to replicate, and any special conditions that should be performed when replicating content.
Replication list	A list of the objects to be replicated. A replication list refers to other content such as users, groups, reports, and so on, in the BI platform deployment to be replicated together.
Replication object	An object that is replicated from an origin site to a destination site. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon.
Replication package	Created during the transfer, the replication package contains objects from a replication job. It can contain all the objects defined in the replication list, as in the case of a rapidly changing environment or initial replication. Or it can contain a subset of the replication list if the objects change infrequently compared to the schedule of the replication job. The replication package is implemented as a BI Application Resource (BIAR) file.
Replication refresh	All objects in a replication list are refreshed regardless of the last modified version.
Two-way replication	Acts the same as one-way replication, but two-way replication also sends changes in both directions. Updates to the origin site are replicated to each destination site. Updates and new objects on a destination site are sent to the origin site.

26.3 Managing security rights

Federation replicates content between separate deployments and requires collaboration with other administrators, therefore it is necessary to understand security before you begin using Federation.

Administrators in separate deployments must coordinate with each other before enabling Federation. After content is replicated, administrators can change content.

Specific rights on the origin and destination deployments are required to accomplish certain tasks:

- Rights required on the origin site
- Rights required on the destination site
- Rights required on Federation-specific objects
- Federation scenarios

> → Tip
>
> It is recommended that you read this chapter prior to enabling Federation.

26.3.1 Rights required on the origin site

This section describes the actions on the origin site and the required rights of the user account connecting to the origin site. This is the account you enter in the remote connection object on the destination site.

Action	Description	Rights required
One-way replication	Performs replication only from the origin site to the destination site. **Note** "View" and "Replicate" rights are required on all objects being replicated, including objects that are automatically replicated by dependency calculations.	• "View" and "Replicate" rights on all objects you want to replicate • "View" right on the replication list
Two-way replication	Performs replication from the origin site to the destination site, and from the destination site to the origin site.	• "View" and "Replicate" rights on all objects you want to replicate • "View" right on the replication list • "Modify Rights" right on user objects to replicate any password changes
Scheduling	Allows remote scheduling to occur on the origin site from the destination site.	• "Schedule" right for all objects that you want to remotely schedule

Related Information

Rights required on the destination site [page 886]

26.3.2 Rights required on the destination site

This section describes actions applied to the destination site and the required rights of the user account that is running the replication job. This is the account of the user who created the replication job.

Note

Like other schedulable objects, you can schedule the replication job on behalf of someone else.

Action	Description	Rights required
All objects	Replicates objects regardless of one-way or two-way replication.	• "View", "Add", "Edit", and "Modify Rights" rights on all objects

Action	Description	Rights required
		• "Modify User Password" right, for all user objects
First replication	The first time the replication job is run, no objects exist on the destination site yet. Therefore, the user account that the replication job is running under must have rights for all top-level folders and objects that will have content added to them.	• "View", "Add", "Edit", and "Modify Rights" rights on all top-level folders and default objects

Related Information

Rights required on the origin site [page 886]

26.3.3 Federation-specific rights

This section details scenarios that are specific to Federation.

Action	Description	Rights required
Object cleanup	Object cleanup deletes objects on the destination site.	• The account that the replication job is running under requires "Delete" rights on all objects that may be potentially deleted.
Disable cleanup for certain objects	When certain objects are replicated from the origin site, you may not want to delete them from the destination site if they are deleted on the origin site. You can safeguard this through rights. For instance, choose this option when users on the destination site start are using an object independently of users on the origin site. For example, in a replicated universe where users on the destination site create their own local reports using this universe, you may not want to lose the universe on the destination site if it is deleted from the origin site.	• Deny "Delete" rights of the user account the replication job is running under on the objects you want to keep.

Action	Description	Rights required
Two-way replication with no modifications on the origin site	In certain circumstances you may choose two-way replication but do not want some objects on the origin site modified, even if they are changed on the destination site. Reasons for this include: if the object is special and should only be changed by users on the origin site; or if you want to enable remote scheduling but do not want changes propagated back. **Note** For remote scheduling, you can create a job that only handles objects for remote scheduling. However, in this case ancestor objects are still replicated, including the report, the folder containing the report, and the parent folder of that folder. Any changes made on the destination site are replicated to the origin site, and changes made on the origin site are replicated to the destination site.	• Deny "Edit" rights of the user account used to connect in the remote connection object.

26.3.4 Replicating security on an object

To keep security rights for an object, you must replicate both the object and its user or group at the same time. If not, they must already exist on the site you are replicating to and have identical unique identifiers (CUIDs) on each site.

If an object is replicated and the user or group is not replicated, or does not already exist on the site you are replicating to, their rights will be dropped.

Example

Group A and Group B have rights assigned on Object A. Group A has "View" rights and Group B has "Deny View" rights. If the replication job replicates only Group A and Object A, then on the destination site, Object A will have only the "View" rights for Group A associated with it.

When you replicate an object, there is a potential security risk if you do not replicate all groups with explicit rights on the object. The previous example highlights a potential risk. If User A belongs to both Group A and Group B, the user will not have permission to view Object A on the origin site. However, User A will be replicated

to the destination site because he belongs to both groups. Once there, because Group B was not replicated, User A will have the right to view Object A on the destination site, but cannot view Object A on the origin site.

Objects that reference other objects that are not included in a replication job, or those not already on the destination site, are displayed in a log file. The log file shows that the object referenced the unreplicated object and dropped its reference.

Security on an object for a particular user or group is replicated only from the origin site to the destination site. You can set security on replicated objects on the destination site, but those settings will not be replicated to the origin site.

26.3.5 Replicating security using access levels

To persist, rights must be defined by access levels. The object, user or group, and access level must be replicated at the same time, or they must already exist on the site you are replicating to.

Objects that assign explicit rights to a user or group that are not included in the replication job, or not already on the destination site, are displayed in its log file, which shows the object had rights assigned that were not replicated and those rights were dropped.

In addition, you can choose to automatically replicate “Access Levels” that are used on an imported object. This option is available on the replication list.

> **Note**
>
> Default access levels are not replicated, but references are maintained.

26.4 Replication types and mode options

Depending on your selection of replication type and replication mode, you may create one of four different replication job options:

- One-way replication
- Two-way replication
- Refresh from origin
- Refresh from destination

26.4.1 One-way replication

With one-way replication, you can replicate content in only one direction, from the origin site to a destination site. Any changes you make to objects on the origin site in the replication list are sent to the destination site. However, changes you make to objects on a destination site are not sent back to the origin site.

One-way replication is ideal for deployments with one central BI platform deployment where objects are created, modified, and administered. Other deployments use the content of the central deployment.

To create one-way replication, select the following options:

- Replication type = One-way replication
- Replication mode = Normal replication

26.4.2 Two-way replication

With two-way replication, you can replicate content in both directions between the origin and destination sites. Any changes made to objects on the origin site are replicated to destination sites, and changes made on a destination site are replicated to the origin site.

> **Note**
>
> To perform remote scheduling and to replicate locally run instances back to the origin site, you must select two-way replication mode.

If you have multiple BI platform deployments where content is created, modified, administered, and used at both locations, two-way replication is the most efficient option. It also helps synchronize the deployments.

To create two-way replication, select the following options:

- Replication Type = Two-way replication
- Replication Mode = Normal replication

Related Information

Remote scheduling and locally run instances [page 915]

26.4.3 Refresh from origin or refresh from destination

When you replicate content in one-way or two-way replication modes, the objects on the replication list are replicated to a destination site. However, not all of the objects may replicate each time the replication job runs.

Federation has an optimization engine designed to help finish your replication jobs faster. It uses a combination of the object's version and time stamp to determine if the object was modified since the last replication. This check is done on objects specifically selected in the replication list and any objects replicated during dependency checking.

However, in some cases the optimization engine may miss objects, which won't be replicated. In these cases, you can use “Refresh from Origin” and “Refresh from Destination” to force the replication job to replicate content, and their dependencies, regardless of the timestamps.

"Refresh from Origin" only sends content from the origin to the destination sites. "Refresh from Destination" only sends content from the destination sites to the origin site.

Example

The following three examples describe scenarios using “Refresh from Origin” and “Refresh from Destination” where certain objects will be missed due to the optimization.

Scenario 1: The addition of objects that contain other objects into an area that is being replicated.

Folder A is replicated from the origin site to the destination site. It now exists on both sites. A user moves or copies Folder B with Report B, into Folder A on the origin site. During the next replication, Federation will see that Folder B's timestamp has changed and will replicate it to the destination site. However, Report B's timestamp does not change. Therefore, it will be missed by a regular one-way or two-way replication job.

To ensure Folder B's content is properly replicated, a replication job with “Refresh from Origin” should be used once. After this, the regular one-way or two-way replication job will replicate it properly. If this example is reversed and Folder B is moved or copied on the destination site, then use “Refresh from Destination”.

Scenario 2: The addition of new objects using LifeCycle Manager or the BIAR command line.

When you add objects to an area that is being replicated using LifeCycle Manager or BIAR command line, the object may not be picked up by a regular one-way or two-way replication job. This occurs because the internal clocks on the source and destination systems may be out of sync when using the LifeCycle Manager or BIAR command line.

> ⓘ Note
>
> After importing new objects into an area that is being replicated on the origin site, it is recommended that you run a “Refresh from Origin” replication job. After importing new objects into an area that is being replicated on the destination site, it is recommended that you run a “Refresh from Destination” replication job.

Scenario 3: In between scheduled replication times.

If you add objects to an area that is being replicated and can't wait until the next scheduled replication time, you can use “Refresh from Origin” and “Refresh from Destination” replication jobs. By selecting the area where objects have been added, you can replicate content quickly.

> ⓘ Note
>
> This scenario can be costly for large replication lists, so it is recommended that you do not use this option often. For example, it is not necessary to create replication jobs to refresh from the origin to destination mode on an hourly schedule. These modes should be used in “run now” or infrequent schedules.

> ⓘ Note
>
> In some cases, you cannot use conflict resolution, including: “Refresh from Origin”: destination site option wins is blocked, or “Refresh from Destination”: origin wins option is blocked.

26.5 Replicating third-party users and groups

In Federation you can replicate third-party users and groups, specifically Active Directory (AD) and LDAP users and groups.

> → Tip
>
> Read this section if you plan to replicate these types of users and groups or their personal content, such as favorite folders or Inboxes.

Mapping users and groups

1. Map the users and groups on the origin site for Federation to replicate them properly.
2. Replicate the mapped users and groups to the destination site.

> ⓘ Note
>
> Do not map groups and users separately on the destination site. If you do, they will have different unique identifiers (CUIDs) on the destination and origin sites, and Federation will not be able to match the user or groups.

Example

The administrator maps Group A with User A on the origin and destination sites. Both Group A and User A have different unique identifiers on the origin and destination sites. During replication, Federation cannot match them and Group A or User A are not replicated due to an alias conflict.

> ⓘ Note
>
> Before replicating third-party users and groups, the destination site must be set up to use AD or LDAP authentication. However, you must also configure the destination site to use AD or LDAP so it can communicate to the directory server or domain controller.

> ⓘ Note
>
> After replicating an AD or LDAP group for the first time, users in this group are unable to log on until the AD/LDAP Group Graph has been refreshed. This occurs automatically approximately every 15 minutes. To refresh AD/LDAP Group Graph manually, go to the *Authentication* page of the CMC, double-click *Windows AD* or *LDAP*, and then click *Update*.

> ⓘ Note
>
> Be careful when replicating third-party groups. When you add new users to the group in the directory server, they will be able to log on to both sites. This security issue of AD or LDAP authentication is independent of Federation.

If you log on to the destination and origin sites separately, or the group membership is updated on both sites using the update button on the CMC authentication page, a user account is created on both sites. The accounts will have different unique identifiers and Federation won't be able to replicate them properly.

It is important to create the account on one site and then replicate it to the other.

26.6 Replicating universes and universe connections

When using Federation to replicate Universes between BI platform deployments, it is important to plan in advance. A Universe object cannot function without an underlying Universe Connection.

Universe Connection objects contain information required to connect to a reporting database. To function correctly, Universe Connection objects must contain valid information and allow a database connection to be established.

> ⓘ Note
>
> If you are using two-way replication and replicate a Universe from the origin site to the destination site without its Universe Connection, in subsequent replications the origin site's Universe may have its relationship to the Universe Connection on the origin site overwritten or removed. To avoid this, always replicate the Universe Connections with the Universes.

To ensure that dependent Universe Connections are replicated with the Universes, always select the following options when you create or modify the replication list that contains the Universes:

- *Include connections used by selected universes*
- *Include universes required by selected universes*

> ⓘ Note
>
> If a Universe's relationship with its Universe Connection has been overwritten or removed, open the Universe, and under *File* > *Parameters*, modify the connection information.

The following two examples demonstrate the process of replicating Universes and their related Universe Connections.

Example

When replicating Universes and Universe Connections, you must ensure that the connectivity environment on the origin site matches the connectivity environment on the destination site.

For example, if the Universe Connection uses an ODBC connection called “TestODBC”, then there needs to be a correctly configured ODBC connection called “TestODBC” on the destination environment. The ODBC connection can resolve to the same database or to a different database. To ensure that Universes using this connection do not encounter connectivity issues, the schemas of the databases must be the same.

Example

If you want the replicated Universe on the destination site to use a different database than the Universe on the origin site uses, replicate the Universe Connection, but have the connectivity information on the destination site point to the desired database.

For example, if the Universe Connection on the origin site is using an ODBC connection called “Test” pointing to “DatabaseA”, make sure you have an ODBC connection on the destination site that is also called “Test” but pointing to “DatabaseB”.

26.7 Managing replication lists

Replication lists include content, such as users, groups, and reports in the BI platform deployment, that can be replicated together. Replication lists are accessed from the CMC.

Content types that can be replicated are explained in the following table.

Category	Supported objects
Repository objects	Objects that include Business Views, DataConnection, LOVs, Data Foundation, and more. **Note** All objects are supported, although not at the individual level.
Reports	Crystal reports, Web Intelligence documents, and Dashboards objects. **Note** Full Client Add-in and templates are supported.
Third-party objects	Excel, PDF, PowerPoint, Word, text files, rich text files, Shockwave files.
Users	Users, groups, Inboxes, Favorites, personal Category.
Business Intelligence Platform	Folders, events, categories, calendars, custom roles, hyperlinks, shortcuts, programs, profiles, object packages, agnostic.
Universes	Universes, connections, universe overload.

Note

The following objects must be created on the origin site and then replicated to the destination site. If you create these objects on the destination site and then replicate them to the origin site, they will not function on the origin site.

- Business Views
- Business Elements

- Data Foundations
- Data Connections
- Lists of Values
- Universe Overloads

26.7.1 Creating replication lists

Context

Replication lists are located in the Replication Lists area of the CMC. You can organize replication lists in folders and subfolders that you create.

26.7.1.1 To create a replication list folder

Procedure

1. Go to the *Replication Lists* area of the CMC.
2. Click *Replication Lists*.
3. Click *Manage* > *New* > *Folder*.
   The *Create Folder* dialog box appears.
4. Type a folder name and click *OK*.
   You can now create replication lists in this folder.

26.7.1.2 To create a replication list

Procedure

1. Go to the *Replication Lists* area of the CMC.
2. Select the folder where you want to save your new replication list.
3. Click *Manage* > *New* > *New Replication List*.
   The *New Replication List* dialog box appears.
4. Type the title and description of the replication list.
5. For advanced options, click the *Replication List Properties* link.

   This allows you to specify which dependencies to automatically replicate from the origin site to the destination site.
6. Select the required options as described in the table.

Dependency object options	Definition
Include personal folders for selected users	Replicates a selected user's personal folders and their content.
Include personal categories for selected users	Replicates a selected user's personal categories.
Include universes for selected reports	Replicates any universe that selected report objects depend on.
Include members of selected user groups	Replicates users within a selected group.
Include universes required by selected universes	Replicates any universes that depend on other universes.
Include inboxes for selected users	Replicates a selected user's Inbox and its content.
Include user groups for selected universes	Replicates the user groups associated with a universe's overloads.
Include access levels set on selected objects	Replicates any access levels used on any of the selected objects.
Include documents for selected categories	Replicates any documents, including Word, Excel, and PDF, that are included in selected categories.
Include profiles for selected users and user groups	Replicates any profiles associated with selected users or groups.
Include connections used by selected universes	Replicates any universe connection objects used by selected objects.

> **Note**
>
> Some objects in the BI platform are dependent on other objects. For example, a Web Intelligence document is dependent on the underlying universe for its structure and content. If you replicate a Web Intelligence document but do not select the universe it uses, replication will not work on the destination site unless the universe was already replicated there. However, if you enable *Include universes for selected reports*, Federation automatically replicates the universes that the report depends on.

7. Click *Next*.
8. Select one or more objects to add to your replication list.
   - Use the arrow buttons to add or remove objects in the *Available Objects* folder.
   - Or, click *Repository objects* under *Replicate all* to replicate all Business View, Business Elements, Data Foundation, Data Connection, List of Values, and repository objects, including report images and functions.

   > **Note**
   >
   > It is not possible to replicate top level folders located in the *Available Objects* folder.
9. Click *Save & Close*.

26.7.2 Modifying Replication Lists

Context

After you create a replication list, you can modify its properties or objects.

26.7.2.1 To modify properties in a replication list

Procedure

1. Go to the *Replication Lists* area of the CMC.
2. Select the *Replication List* you want to modify.
3. Click *Manage* > *Properties*.
   The *General Properties* dialog box appears.
4. Modify the title and description. You can also modify the other areas of the replication list while the *General Properties* dialog box is open.
5. If you want to modify dependency options, click *Replication List Properties* on the navigation list.
6. Click *Save & Close*.

Related Information

Creating replication lists [page 895]

26.7.2.2 To modify objects in a replication list

Procedure

1. Go to the *Replication Lists* area of the CMC.
2. Select a *Replication List*.
3. Click *Actions* > *Manage Replication List*.
   The *Manage Replication List* dialog box appears with a list of objects included in the replication list.
4. Add or remove objects as desired.
5. Click *Save & Close*.

Related Information

Creating replication lists [page 895]

26.8 Managing remote connections

Context

Remote connection objects contain the information needed to connect to a remote BI platform deployment.

> **Note**
>
> The remote connection object is created on a destination site BI platform deployment. The remote connection is the origin site.

You can view remote connections in the *Federation* area of the CMC.

26.8.1 Creating remote connections

Prerequisites

A remote connection in Federation connects to a remote BI platform deployment. To establish a connection to the origin site where the content to be replicated is located, you must first create a remote connection on the destination site.

Context

You can create folders and subfolders to organize your remote connections.

26.8.1.1 To create a remote connection folder

Procedure

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Click *Manage* > *New* > *Folder*.

A *Create Folder* dialog box appears.

4. Type a folder name and click *OK*.
   You can now create remote connections in this folder.

26.8.1.2 To create a remote connection

Context

To connect to a remote BI platform deployment, you must create a remote connection in Federation.

Procedure

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Click *Manage* > *New* > *New Remote Connection*.
   The *New Remote System Connection* dialog box appears.
4. Enter a title, description, and related fields as required:

> **Note**
>
> All fields are mandatory, except “Description” and “Limit the number of cleanup objects”.

Field	Description
Title	Name of the remote connection object.
Description	Description of the remote connection object. (Optional)
Remote System Web Service URI	URL to Federation Web Services, which is automatically deployed on your Java application server. You can use any Federation Web Services in the BI platform whether they are the origin or destination site, or another deployment. Use this format: `http://<application_yourserver_machine_name>:<port>/dswsbobje`. Example: `http://<mymachine.mydomain.com>:<8080>/dswsbobje`

Field	Description
Remote System CMS	The name of the CMS you want to connect to that is accessible through Federation Web Services. This will be treated as the CMS for the origin site. This is the format: **`CMS_Name:port`**. Example: **`<mymachine>:6400`** **Note** If you are using the default port 6400, specifying the port is optional.
User Name	The user name that is used to connect to the origin site. **Note** Ensure that the user name you are using has view rights on the replication list at the origin site deployment.
Password	The password of the user account to connect to the origin site.
Authentication	The type of account authentication to connect to the origin site. Options are: Enterprise, AD, or LDAP.
Cleanup Frequency (in hours)	How often replication jobs that use this remote connection object perform an object cleanup. Enter only positive whole numbers. The unit is hours. Default = 24.
Limit the number of cleanup objects to	The number of objects a replication job cleans up. (Optional)

5. Click *OK*.

26.8.2 Modifying remote connections

Context

After you create a remote connection, you can modify its properties and security options.

To modify a remote connection:

Procedure

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Double-click the remote connection you want to modify.
   The *Remote Connection Properties* dialog box appears. You can modify the following properties:
   - *Title*
   - *Description*
   - *Remote System Web Service URI*

- *Remote System CMS*
- *User Name*
- *Password*
- *Authentication*
- *Cleanup Frequency (in hours)*
- *Limit the number of cleanup objects to*

4. Specify your changes.
5. Click *Save & Close*.

26.9 Managing replication jobs

Context

A replication job is a type of object that runs on a schedule and is used to replicate content between two BI platform deployments in federation.

> **Note**
>
> Replicated objects on a destination site will be flagged with a replication icon as shown here: If there is a conflict, an object will be flagged with a conflict icon as shown here:

You can view a list of replication jobs in the *Remote Connection* folder in the *Federation* area of the CMC.

26.9.1 Creating replication jobs

Context

A replication job is required to replicate content between two BI platform deployments in federation. Each replication job must have only one remote connection and one replication list associated with it.

26.9.1.1 To create a replication job

Procedure

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Select a *Remote Connection* to contain the new replication job.

> ⚠ Caution
>
> The CMC must be able to connect to Web Services in the remote connection URI to continue using the wizard.

4. Click *Manage* > *New* > *New Replication Job*.
   A *New Replication Job* dialog box appears.
5. Type a title and description of the replication job.
6. Click *Next*.
   A list of available replication lists on the origin site appears.
7. Select the *Replication List* you want to use with your replication job.
8. Click *Next*.
9. Select configuration options as described in the table below.

Option	Description
Enable object cleanup on destination	Forces the replication job to delete any replicated objects on the destination site, where the originating object on the origin site was removed. ⓘ Note Object Cleanup will not delete objects replicated using dependencies or objects selected on the replication list.
One-way replication	Specifies that an object only replicates from the origin site to the destination site. Any changes made after replication to the object on the origin site are replicated to the destination site, but changes made on the destination site are not replicated back to the origin site.
Two-way replication	Specifies that objects are replicated in both directions; from the origin site to the destination site, and from the destination site to the origin site. Changes made to these objects after replication at one site are then automatically replicated to the other site.
Origin site takes precedence	Specifies that when a conflict is detected between an object on the origin site and its replicated version on the destination site, the version on the origin site takes priority.
No automatic conflict resolution	Specifies that no action is taken to resolve any detected conflicts.
Destination site takes precedence (Only available with two-way replication)	Specifies that when a conflict is detected between an object on the origin site and its replicated version on the destination site, that the version on the destination site takes priority.
Normal replication	Specifies that the replication job acts normally.
Refresh from origin	Replicates all content from the origin site to the destination site whether it has changed or not. You can replicate the entire replication list or only a portion of it.

Option	Description
Refresh from destination (Only available with two-way replication)	Replicates all content from the destination site to the origin site whether it has changed or not. You can replicate the entire replication list or only a portion of it.
Replicate all objects (Only visible with two-way replication)	Replicates the entire replication list. **Note** This is the most complete option but takes the longest to perform.
Replicate remote schedules (Only visible with two-way replication)	Replicates pending remote instances from the destination site to the origin site, and forces completed instances from the origin site to the destination site.
Replicate document templates	Replicates all objects that aren't instances (locally run or reports that are checked for remote scheduling). This includes users, groups, folders, reports, and so on.
Replicate locally run completed instances	Replicates completed instances only from the destination site to the origin site.

10. Click *OK*.

26.9.2 Scheduling replication jobs

After you create a replication job, you can schedule it to run once or on a recurring basis. You can also schedule multiple replication jobs on one destination site from one origin site.

Note

If you schedule multiple replication jobs on one destination site, only one replication job can connect to the origin site at a time. All other replication jobs that try to connect will be moved to a pending state and remain pending until they are able to automatically connect to the origin site.

26.9.2.1 To schedule a replication job

Procedure

1. Go to the *Federation* area of the CMC.
2. Select the *Replication Job* you want to schedule.
3. Click *Actions* > *Schedules*.
4. Select the desired scheduling options.

26.9.3 Modifying replication jobs

Context

After you create a replication job in Federation, you can modify its properties.

26.9.3.1 To modify a replication job

Procedure

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections* folder.
3. Select the *Remote Connection* object that contains the *Replication Job* you want to modify.
4. Select the *Replication Job* you want to modify.
5. Click *Manage* > *Manage object properties*.
6. View and edit the *Properties*, *Schedule*, *History*, *Replication List*, and *User Security*, as necessary.

Sections	Description
Properties	Modify the name, description and other general properties and options of the replication job.
Schedule	Set the replication job to run on a recurring schedule.
History	View and administer all instances of the replication job.
Replication List	Change the selected replication list.
User Security	Set rights on the replication job.

26.9.4 Viewing a log after a replication job

Context

Every time you run a replication job, Federation automatically produces a log file, which is created on the destination site. The log files use XML 1.1 standards and require a web browser that supports XML 1.1.

To view a replication log:

Procedure

1. Go to the *Federation* area of the CMC.
2. Click *All Replication Jobs*.
3. Select a *Replication Job* from the list.
4. Click *Properties*.
   The replication job *Properties* page opens.
5. Click *History*.
6. Click the *Instance time* of the log file to view successful replication jobs, or click *Failed* status to view a log file of failed replication jobs.
7. Select desired instance to view the log file.
   The log file is generated in XML format and uses an XSL form to format the information into an HTML page.

   You can access the XML log from the computer that is running the Server Intelligence Agent that contains the Adaptive Job Server. You can find the log file at this location:

   - On Windows: `<InstallDir>\SAP BusinessObjects XI 4.0\logging`
   - On Unix: `<InstallDir>/sap_bobj/logging`

26.10 Managing object cleanup

In Federation, you should perform object cleanup throughout the lifecycle of your replication process, to make sure all objects that you delete from the origin site are also deleted from each destination site.

Object cleanup involves two elements: a remote connection and a replication job. A remote connection object defines general cleanup options, and a replication job performs the clean up when the appropriate interval passes.

26.10.1 How to use object cleanup

Separate replication jobs that use the same remote connection work together during object cleanup. This means that your replication job will clean up objects within its replication list, as well as objects within other replication lists that use the same remote connection. A remote connection is only considered the same if the parent of the replication job is the same remote connection object.

Example

Replication Jobs A and B replicate Object A and Object B. They both replicate from the same origin site and use the same remote connection. If the origin site deletes Object B , Replication Job A will see that Object B was deleted. Even though Replication Job B is the one replicating it, Object B will also be removed from the destination site. When Replication Job B executes it won't need to run an object cleanup.

> ⓘ Note
>
> Only objects on the destination site are deleted during object cleanup. If you remove an object from the origin site that is part of a replication, the object will be removed from the destination site. However, if an object is removed from the destination site, it will not be removed from the origin site during object cleanup, even if the replication job is in two-way replication mode.
>
> Objects that are deleted or removed from the replication list are not deleted from destination site. To properly remove an object that is specified in a replication list, you should delete it on both the destination site and the origin site. Objects that are replicated via dependency calculations are not deleted.

26.10.2 Object cleanup limits

In the remote connection object, you can define the number of objects a replication job will clean up at one time. Federation automatically tracks where the clean up job ends. This way, the next time you run a replication job, it starts the next clean up job at that point.

> → Tip
>
> To complete a replication job faster, limit the number of objects for cleanup.

Example

Replication Jobs A and B are replicating Object A and Object B. Both objects are replicated from the same origin site and use the same remote connection.

If the origin site deletes Object B and the object limit is set to 1, the next time Replication Job A runs, it will only check if Object A has been deleted. This way, the Object B is not checked and will not be deleted.

Next, Replication Job B runs and starts the object cleanup at the point where Replication Job A ended. It will check if Object B has been deleted and remove it from the destination site. You can find this option on the remote connection object's property “Limit the number of clean up objects to:”

> ⓘ Note
>
> If you do not select this option, all replication jobs that use this remote connection will check all objects for potential clean up.

26.10.3 Object cleanup frequency

You can set the how often a replication job performs object cleanup in the remote connection “Cleanup Frequency” field.

> **Note**
>
> You must enter a positive whole number, which represents the number of hours to wait between object cleanup processing.

Example

Replication Jobs A and B replicate Object A and Object B. Both objects are replicated from the same origin site and use the same remote connection.

If Object B is deleted from the origin site and all of the following conditions are true, the replication job will check if Object A has been deleted.

- The Object Limit is 1
- The cleanup frequency is 150 hours
- Replication Job A runs next

Because the object limit is 1, Object B will not be checked or deleted on the destination site.

The next cleanup occurs 150 hours after Replication Job A did the initial check. Although Replication Jobs A and B may execute many times before the 150 hour limit, neither will attempt to run an object cleanup. After 150 hours, the next replication job will execute and attempt cleanup. Then it will determine that Object B was deleted on the origin site, and then delete it on the destination site.

Enabling and disabling options

Each replication job can participate in object cleanup. Use "Enable Object Cleanup on destination" option on a replication job to instruct it whether to run an object cleanup. In some cases, you may have high priority replication jobs you do not want to participate in object cleanup, so you can execute them as quickly as possible. To do this, disable object cleanup.

Related Information

Object cleanup limits [page 906]

26.11 Managing conflict detection and resolution

In Federation, a conflict can occur when the properties of an object are changed on both the origin site and destination site. Both top level and nested properties of an object are checked for conflicts. For example, a conflict can occur if a report or the name of a report is modified on both the origin and destination sites.

Some instances do not create a conflict. For example, if the name of a report is modified on the origin site, and the description of the replicated version is modified on the destination site, the changes merge together and no conflict occurs.

26.11.1 One-way replication conflict resolution

In one-way replication, you have two choices for conflict resolution.

Origin site takes precedence

If a conflict occurs during one-way replication, the origin site object takes precedence. Any changes to objects on a destination site are overwritten by the origin site's information. For example, if a report is modified on both the origin site and the destination site, the destination site modification will be overwritten by the origin site version after the next replication job.

> **Note**
>
> Because the conflict is automatically resolved, it is not generated in the log file and does not appear in the conflicting object list.

No automatic conflict resolution

If a conflict occurs and you select "No automatic conflict resolution", the conflict is not resolved, a log file is not generated, and it does not appear in the conflicting object list.

Administrators can access a list of all replicated objects that are in conflict in the Federation area of the CMC. Objects in conflict are grouped together by the remote connection they used to connect to the origin site with. To access these lists, go to the Replication Errors folder in the Federation area of the CMC, and select the desired remote connection. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon. A warning message also appears in the *Properties* page.

> **Note**
>
> The list is updated when a replication job that uses a remote connection is completed. It contains all objects in conflict for all of the replication jobs that use its specific remote connection.

> **Note**
>
> Any user with access to the CMC and the replication job instances can access the XML log saved in the logfile directory. A destination site object's icon is flagged to indicate a conflict. During processing, a conflict log is created.

Abdul modifies Report A on the origin site. Maria modifies the replicated version on the destination site. The next time the replication job runs, the report will be in conflict as it has changed on both sites and it will not be resolved.

The destination report is maintained and changes to the origin's report are not replicated. Subsequent replication jobs will behave the same way until the conflict is resolved. Any changes on the origin site are not replicated until the conflict is manually resolved.

> **Note**
>
> In this case, the entire object is not replicated. Other changes that may not be in conflict are not brought over.

To manually resolve a conflict, you have three options:

1. Create a replication job that replicates only the objects in conflict. It must use the same remote connection object and replication list.
   To keep the origin site changes, create a replication job. Then set replication mode to "Refresh from Origin", and set Automatic Conflict Resolution to "Origin site takes precedence".
   To keep the destination site changes, create a replication job with Replication Type = "Two-way replication", Replication Mode = "Refresh from Destination", and Automatic Conflict Resolution = "Destination site takes precedence"

   > **Note**
   >
   > In replication mode, set "Refresh from Origin " or "Refresh from Destination", to select only the objects in conflict on the replication list. This way, other objects are not replicated. Next, schedule the replication job to run and it will replicate the selected objects and resolve the conflict as specified.
2. Create a replication job that replicates only the objects in conflict. It will need to use the same remote connection object. However unlike option 1, you may create a new replication list on the origin site. Use only the objects in conflict and create a new replication job which will use this focused replication list.
   To keep the origin site changes, set the Automatic Conflict Resolution to "Origin site takes precedence".
   To keep the destination site changes, set Automatic Conflict Resolution to "Destination site takes precedence" and the Replication Type to "Two-way replication".
3. For one-way replication jobs, you may only delete the object on the destination site. The next time the replication job executes, it replicates the object from the origin site to the destination site.

   > **Note**
   >
   > Be careful when deleting an object because other objects that depend on it may be removed, stop working, or lose security. Options 1 and 2 are recommended.

26.11.2 Two-way replication conflict resolution

In two-way replication conflict, you have three choices for conflict detection:

- Origin site takes precedence
- Destination site takes precedence
- No automatic conflict resolution

Origin site takes precedence

If a conflict occurs, the origin site will take precedence and overwrite any changes to the destination site.

Example

Lily modifies the name of a report to Report A. Malik modifies the name of the replicated version on the destination site to Report B. After the next replication job runs, the replicated version on the destination site will revert to Report A.

This will not generate a conflict in the log file, and it will not appear in the conflicting object list because the conflict was resolved according to the user's instructions on the origin site.

Destination site takes precedence

If a conflict occurs, the destination site keeps its changes and overwrites them to the origin site.

Example

Kamal modifies the name of a report to Report A. Peter modifies the name of the replicated version on the destination site to Report B. When the replication job runs, a conflict is detected. The name of the destination report remains as Report B.

In two-way replication, changes are also sent back to the origin site. In this scenario, the origin site is updated and its report name is changed to Report B. This does not generate a conflict in the log file and it will not appear in the conflicting object list because the conflict was resolved according to the user's instructions.

No automatic conflict resolution

When “No automatic conflict resolution” is selected, a conflict will not be resolved. The conflict will be noted in a log file for the administrator, who can manually resolve it.

> **Note**
>
> An object's icon is flagged to indicate that a conflict exists.

> **Note**
>
> Although changes are replicated to both origin and destination sites in two-way replication, only the destination site's versions will be flagged with a conflict icon.

> **Note**
>
> Any user with access to the CMC and the replication job instances can access the XML log outputted in the logfile directory. A destination site object's icon is flagged to indicate a conflict. During processing, a conflict log is created.

The administrator can access a list of all replicated objects that are in conflict in the Federation area of the CMC. Objects in conflict are grouped together by the remote connection they used to connect to the origin site with. To access these lists, go to *CMC* > *Federation* > *Replication Errors* > *Remote Connection*.

> **Note**
>
> The list is updated when a replication job that uses a remote connection is completed. It contains all objects in conflict for all of the replication jobs that use its specific remote connection. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon.

Example

Michael modifies Report A on the origin site. Damien modifies the replicated version on the destination site. When the next replication job runs, the report is in conflict as it has changed on both sites and will not be resolved.

The destination report is kept and changes to the origin's report are not replicated. Subsequent replication jobs behave the same way until the conflict is resolved. Any changes on the origin site will not get replicated until the conflict is manually resolved by the administrator or delegated administrator.

> **Note**
>
> In this case, the entire object is not replicated. Other changes that are not in conflict are not replicated.

> **Note**
>
> Any user with access to the CMC and the replication job instances can access the XML log outputted in the logfile directory. A destination site object's icon is flagged to indicate a conflict. During processing, a conflict log is created.

The administrator can access a list of all replicated objects that are in conflict in the Federation area of the CMC. Objects in conflict are grouped together by the remote connection they used to connect to the origin site with. To access these lists, go to *CMC* > *Federation* > *Replication Errors* > *Remote Connection*.

> **Note**
>
> The list is updated when a replication job that uses a remote connection is completed. It contains all objects in conflict for all of the replication jobs that use its specific remote connection. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon.

To manually resolve a conflict, you have three options:

1. Create a replication job that replicates only the objects in conflict. It must use the same remote connection object and replication list.
   To keep the origin site changes, create a replication job. Then set the Replication Mode to “Refresh from Origin” and set Automatic Conflict Resolution to “Origin site takes precedence”.
   To keep the destination site changes, create a replication job and set Replication Type to “Two-way replication”, set Replication Mode to “Refresh from Destination”, and set Automatic Conflict Resolution to “Destination site takes precedence”.

   > ⓘ Note
   >
   > In Replication Mode, set “Refresh from Origin” or “Refresh from Destination”, to select only the objects in conflict on the replication list. This way, other objects are not replicated. Next, schedule the replication job to run and it will replicate the selected objects and resolve the conflict as specified.

2. Create a replication job that replicates only the objects in conflict. It will need to use the same remote connection object. However unlike option 1, you may create a new replication list on the origin site. Use only the objects in conflict and create a new replication job, which will use this focused replication list.
   To keep the origin site changes, set the Automatic Conflict Resolution to: “Origin site takes precedence”.
   To keep the destination site changes, set Automatic Conflict Resolution to: “Destination site takes precedence” and the Replication Type to: “Two-way replication”.
3. Delete the object on the site you don't want it to be located.

> ⓘ Note
>
> Be careful when deleting an object because other objects that depend on it may be removed, stop working, or lose security. Options 1 and 2 are recommended.

To keep the destination site changes, you can delete the object on the origin site. The next time the replication job executes, it replicates the object from the destination site to the origin site.

> ⓘ Note
>
> Be careful when deleting a origin site's copy as other destination sites that replicate that object may execute their replication job before the copy has been replicated back. This will cause the other destination sites to delete their copy, which will be unavailable until the copy is returned.

To maintain the origin site changes, you can delete the object on the destination site.

26.12 Using Web Services in Federation

Federation uses Web Services to send objects and their changes between the origin and destination sites. Federation-specific web services are automatically installed and deployed in your BI platform installation. However, you may want to modify properties or customize deployments in Web Services to improve functionality, as described in this section.

> → Tip
>
> To improve file management and functionality, enable file caching in Federation.

26.12.1 Session variables

If you are transferring a large number of content files in one replication job, you may want to increase the session timeout period of the Federation Web Services.

The property is located in the `dsws.properties` file:

`<App Server Installation Directory>\dswsbobje\Web-INF\classes`

For example:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\classes
```

To activate a session variable, enter:

```
session.timeout = x
```

Where “x ”is the desired time, “x” is measured in seconds. If not specified, the default value is 1200 seconds or 20 minutes.

The new properties take effect only after the modified web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

26.12.2 File caching

File caching allows Web Services to handle very large attachments without buffering them in memory. If it is not enabled during large transfer sizes, all of the Java's Virtual Machine memory can be utilized and replication may fail.

> **Note**
>
> File caching decreases performance as the Web Services process to files instead of memory. You may use a combination of both options and send large transfers to a file and smaller ones into memory.

To enable file caching, modify the `Axis2.xml` file located at:

`<App Server Installation Directory>\dswsbobje\Web-Inf\conf`

For example:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
```

Enter the following:

```
<parameter name="cacheAttachments" locked="false">true</parameter>
<parameter name="attachmentDIR" locked="false">temp directory</parameter>
<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> **Note**
>
> Threshold size is measured in bytes.

The new properties take effect only after the modified web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

26.12.3 Custom deployment

Federation Web Services may deploy automatically and require the “federation”, “biplatform”, and “session” services to activate. To disable Federation or any other Web Services, modify the corresponding Web Services `service.xml` file.

BI platform Web Services are located in:

```
<App Server Installation Directory>\dswsbobje\WEB-INF\services
```

Example:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\services
```

To deactivate Web Services:

- add “activate” property in the service name tag of the `service.xml` file and set it to false
- restart your Java application server

For example, to disable Federation:

The `services.xml` file is located in:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\services\federator\META-INF
```

Change the service name from:

```
<service name="Federator">
```

To:

```
<service name="Federator" activate="false">
```

The new properties take effect only after the modified web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

26.13 Remote scheduling and locally run instances

This section describes remote scheduling, locally run instances, and instance sharing. These features allow reports to run where the data resides and send completed instances to the appropriate locations.

26.13.1 Remote scheduling

Using Federation, you can schedule a report on the destination site and then process it on the origin site. The completed instance will be returned to the destination site.

To enable remote scheduling, schedule a report as normal and enable the option “Run at origin site”. To enable this option, click *Schedule* > *Scheduling Server Group* > *Run at origin site*. After the scheduled instances are created, they are placed in the pending stage.

During remote scheduling, information submitted on the destination site is disregarded and the report instance remains in the pending stage.

When the next replication job that manages the report is enabled for remote scheduling, it copies the instance to the origin site for processing. The instance remains in a pending state until the scheduler processes it. Meanwhile, the replication job that sent it will return any previously completed instances and object changes.

Once the instance has processed on the origin site, it reverts to a completed state. When the next replication job that manages the report is enabled for remote scheduling, it uses the completed instance to update the copy on the destination site. Once updated, the instance on the destination site is complete.

> **Note**
>
> A replication job has to run twice to bring back one completed instance.

Example

1. Tom schedules Report A for remote scheduling.
2. Report A is created on the destination site and is in the pending state.
3. Replication Job A runs. First, it replicates changes from the origin site to destination site (including previously completed instances). Second, it copies the instance in the pending state to the origin site, as well as changes to be replicated from the destination site to the origin site.
4. At the origin site, the scheduler picks up the instance in the pending state and sends it to the appropriate job server for processing. The instance is then processed and placed in the completed state on the origin site.
5. Replication Job A runs again. When it replicates content from the origin site to the destination site, the completed instance Report A is picked up and changes are applied to the destination's version.
6. Once this task is done, the destination's version is complete.

Remote scheduling only works with a two-way replication job. You must enable “Replicate remote schedules”. This option is located on the *Replication Job Properties* page in the “Replication Filters” area. In some

scenarios, you may want to replicate remotely scheduled jobs more frequently than other objects on your replication list. To do this, create two replication jobs. Enable one job with “Replicate remote schedules” for a replication job that is only focusing on remote scheduling. Enable the other job with “Replicate document templates” or “Replicate all objects (no filter)”.

> **Note**
>
> When you enable remote scheduling, completed and failed instances appear on both the origin and destination site.
>
> If a user on the destination site schedules a report for remote scheduling and the user does not exist on the origin site, the instance will fail on the origin site. The owner of the failed instance will be the user account of the remote connection object used to connect to the origin.
>
> A replication job may only be configured for remote scheduling, but it always replicates the ancestor objects of the report instance. This means that if there are any changes between replications, it replicates the actual report, reports folder, and so on. If you do not want these changes on the destination site to be replicated to the origin site, you can use security rights to control which changes are replicated.

Related Information

Managing security rights [page 885]

26.13.2 Locally run instances

Locally run Instances are instances of a report that are processed from reports on the destination site. With Federation, you can replicate the completed instances from the destination site to the origin site.

To enable a replication job to replicate completed and failed instances from the destination site to the origin site, click *Replication Job Properties* > *Replication Filters* > *Replicate locally run completed instances*.

In some cases, you may want a replication job to only replicate locally run instances. To do this, enable “Replicate locally run completed instances”.

> **Note**
>
> When you enable locally run Instances on a replication job, both completed and failed instances are replicated to the origin site. This means that there will be copies on both the origin and destination sites.
>
> Pending instances are never replicated.
>
> If the owner of a locally run instance does not exist on the origin site, then the owner will be the user account used to connect in the remote connection object.

26.13.3 Instance share

When you enable Remote Scheduling and Locally Run Instances in a replication job, instance share may occur if one origin site with multiple destination sites are replicating the same report.

Example

Report A originates on the origin site, while destination sites A and B are replicating it. Instance share occurs at both destination sites:

- Enabled replication jobs with "Replicate remote schedules" and/or "Replicate locally run completed instances" Replicate Report A with the same replication job as above
- Schedule Report A on the destination site to "run at origin" and/or to run locally

If both destination sites A and B replicate Report A and their corresponding replication jobs are replicating remote schedules and/or replicating locally run instances, then any instances that were processed at destination site A and/or at the origin site on behalf of destination site A will be shared with destination site B.

Similarly, any instances processed at destination site B and/or processed at the origin site will also be shared with destination site A. Finally, the origin site and destination sites A and B will have an identical set of instances.

Instance share is ideal in many cases. For example, when users from other sites need to access information from their sister deployments. In this case, to prevent instances from being viewed by users at the local site, ensure the proper security rights are set. For example, in a report object, apply the rights so users can see only the instances they own.

> ⓘ Note
>
> All objects follow the BI platform security rules. To ensure that users and groups can only view applicable instances, it is recommended that you set rights so that the users can only view instances that they own. For example, in a report object, apply the rights so users can see only the instances they own.

Related Information

Managing security rights [page 885]

26.14 Importing and promoting replicated content

In some cases, you may choose to import or promote replicated content from one BI platform system to another. This section discusses these features in Federation.

> ⓘ Note
>
> Object migrations are best performed by members of the Administrators group, in particular the Administrator user account. To migrate an object, many related objects may also need to be migrated.

Obtaining the required security rights for all the objects may not be possible for a delegated administrator account.

26.14.1 Importing replicated content

If you use the LifeCycle Manager to import content from one BI platform deployment to another, the LifeCycle Manager does not import any of the replication-specific information associated with replicated objects that are being imported. This means that after the import, the object acts as if it was never replicated. This is specific to replicated objects on a destination site and is described in the following scenario.

Example

BI platform A is a destination site in a Federation process. Report A, a replicated report on System A, is imported from System A to BI platform B using the LifeCycle Manager.

Outcome: When Report A is copied to BI platform B, it doesn't contain any replicated information. Report A will no longer be flagged with a replication icon. If the object was in conflict on BI platform A, it will not be in conflict on System B. Essentially it is treated as an object that originated from System B.

> ⓘ Note
>
> The CUID may or may not be the same, depending on the import choices you select in the LifeCycle Manager.

26.14.2 Importing replicated content and continuing replication

After you've imported replicated content, you may want to include the imported objects in a Federation process. There are two scenarios: treat the system that the imported objects reside on as an origin site, or treat the system as a destination site. To treat this system as an origin site, proceed with Federation as normal.

To treat the system as a destination site and replicate the imported objects from the origin site, you must:

- Ensure the CUID of the objects are preserved when you use the LifeCycle Manager.
- Ensure the first replication job either has conflict resolution set to “Origin wins” or “Destination wins”.

> → Tip
>
> Instead of importing the object using LifeCycle Manager from one destination site to another, it is more efficient and highly recommended to only use Federation to replicate the object.

Example

Report A was created on BI platform System A. System X used Federation to replicate Report A from System A to System X. The LifeCycle Manager then imported Report A from System X to System Y.

Plan: System Y wants to set up Federation to System A, and keep Report A as part of Replication. System Y is the destination and System A is the origin.

Action: When importing Report A from System X to System Y, the CUID of Report A must be preserved. In addition, when the first Replication Job executes, it will try to replicate Report A. Because the object already exists on System Y, replication will produce a conflict. To specify which version to use, you must set the Conflict Resolution mode to either "Origin wins" or "Destination wins".

> ⓘ Note
>
> In this example, it is recommended that instead of importing the object using LifeCycle Manager from one destination site to another, only use Federation to replicate the object. Report A will replicate from System A to System Y and it is unnecessary to use LifeCycle Manager to import from System X to System Y.

26.14.3 Promoting content from a test environment

In any organization, testing is often done before placing anything into a production environment. It is normal to test Federation between BI platform systems in a development or testing environment prior to setting Federation up on your production machines. Once you create your origin site and destination sites and content in a testing environment, you can promote this set up to your production machines using the following steps:

1. Use the LifeCycle Manager to promote your content from your origin site in the testing environment to the machine in production that will act as your origin site.

   > ⓘ Note
   >
   > The replication list object is not selectable when using the LifeCycle Manager.

2. Create the replication list on the origin site in the production environment and include the desired content.
3. Choose from these two following options:
   - A) Create a remote connection object and the appropriate replication jobs on the production machine(s) in production that will act as your destination site(s).
   - B) Use the LifeCycle Manager to import the remote connection and replication jobs from the destination site in Dev/QA to the production machines that will act as destination site(s). Then edit the imported remote connections to point to the machine in production that will act as the origin site.

26.14.4 Re-pointing a destination site

Currently, after an object is replicated from an origin site, it must always be replicated from that origin site and cannot be replicated from another BI platform if the remote connection object is edited to point to a new system, any attempt to replicate an object that was replicated from a different BI platform system than the

remote connection object will fail to replicate. To replicate an object from a different origin site, delete it from the destination site first.

> **Note**
>
> After you copy a replicated object, the CUID of the copy is changed and the copy will not contain any replicated information.

26.15 Best practices

You can use Federation to optimize the performance of a replication job.

If there are a large number of objects in a single replication job, you can take additional steps to ensure that it runs successfully. Typically, you should be able to replicate up to 32,000 objects in each replication job. However, some deployments may require configurations with smaller or larger replication sizes.

1) Obtain a dedicated Web Services provider

In Federation, replicated content is sent using Web Services. In a default installation of the BI platform, all Web Services use the same web service provider. Larger replication jobs may utilize the web service provider longer and slow down its response to other web service requests as well as any applications it serves.

If you plan to replicate a large number of objects at once, or run several replication jobs in sequence, you may consider deploying Federation Web Services on its own Java Application server using your own web services provider.

To do this, use the BI platform installer to install web services. You must have a Java Application Server already running. If you do not, install the entire Web Tier Components option, which will install web services and Tomcat.

> **Note**
>
> You must provide information for an existing CMS (for example, host name, port, and administrator password).

> **Note**
>
> You will need to use this new Web Services provider's URI in your remote connection's URI field.

2) Increase the Java Application Server's available memory

Increase the available memory of your Java Application Server if your single replication job replicates many objects, or if you are sharing the Application Server with other applications.

If you deployed the BI platform and Tomcat, the default available memory is 1 GB. To increase the available memory for Tomcat:

In Windows:

1. Click *Start* > *Programs* > *Tomcat* > *Tomcat Configuration*.
2. Select *Java*.

3. In the *Java Options* box, locate `-Xmx1024M`
4. Increase the `-Xmx1024M` to the desired size.

Example

To increase the memory to 2 GB, enter: `-Xmx2048M`

In Unix:

1. In the `<BOE_Install_Dir>/setup/`, open `env.sh` with your preferred text editor. Increase the `-Xmx1024m` parameter to the desired size.
2. Locate the following lines

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxMetaspaceSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

> **Note**
>
> In BI 4.2 Support Package 5, you can use the MaxMetaspaceSize parameter to define metaspace memory size, as opposed to the MaxPermSize parameter.
>
> - If you are upgrading from versions earlier than BI 4.2 Support Package 5 to BI 4.2 Support Package 5, you need to manually edit the parameter for all existing servers.
> - If you are performing a fresh installation of BI 4.2 Support Package 5, the parameter is replaced by default.

3. Increase the `-Xmx1024m` parameter to the desired size.

Example

To increase the memory to 2 GB, enter: `-Xmx2048m`

> **→ Tip**
>
> For other Java application servers, refer to your Java application server's documentation to increase the available memory.

3) Reduce the size of the BIAR files being created.

Federation uses Web Services to replicate content between the origin site and destination site. Objects are grouped together and compressed into BIAR files for more efficient transportation.

When replicating a large number of objects, configure your Java Application Server to create smaller BIAR files. Federation will package and compress objects across multiple smaller BIAR files so the number of objects you want to replicate will not be limited.

To reduce the size of the BIAR files created, add the following Java parameters to your java application server:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

`bobj.biar.suggestSplit` suggests an appropriate size of the BIAR file, which it will try to meet. Suggested new value is 90MB.

`bobj.biar.forceSplit` will force a BIAR file to stop at a given size. Suggested new value is 100 MB.

> **Note**
>
> You do not need to change the default BIAR file size settings unless your application server is running out of memory and its maximum heap size cannot be increased any further.

For Tomcat Windows:

1. To open the *Tomcat Configuration* tool, click *Start* > *Programs* > *Tomcat* > *Tomcat Configuration*.
2. Select *Java*.
3. In the *Java Options* box, add the following lines at the end:

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

For Tomcat Unix/Linux:

1. Open the env.sh with your preferred text editor. It is located in `<BOE_Install_Dir>/setup/`
2. Locate the following lines:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ];
then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Add the desired BIAR file size parameters.

Example: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

For other Java Application servers, consult your documentation to add Java system properties.

4) Increase the Socket Timeout.

The Adaptive Job Server is responsible for running the replication job. During the execution of the replication job, the Adaptive Job Server establishes a connection to the origin site. When receiving large amounts of information from the origin site, it is important that the Socket which the Adaptive Job Server is using to receive information does not timeout.

The default value is 90 minutes. You can increase the Socket Timeout if you need to.

To increase the Socket Timeout on the Adaptive Job Server:

1. Open the Central Management Console (CMC)
2. Navigate to the *Server* section and select *Adaptive Job Server*.
3. Click *Properties*.
4. Add "Command Line Parameters" to the end of the following:
   - **Windows:** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>`
   - **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>`

Related Information

Troubleshooting error messages [page 924]
Using Web Services in Federation [page 912]
Current release limitations [page 923]

26.15.1 Current release limitations

Federation is a flexible tool, however certain limitations may affect its performance during production. This section highlights areas that you can modify to optimize your Federation operations.

- Maximum number of objects
  Each replication job replicates objects between BI platform deployments. It is recommended that the maximum number of objects you replicate in a single replication job is 100,000. While a replication job may function with more than 100,000 objects, Federation only supports replicating up to 100,000 objects.
- Rights
  In Federation, rights are only replicated from the origin site to the destination site. It is recommended that user rights common to both deployments are set on the origin site and replicated to the destination sites using two-way replication. User rights on a specific site will be administered as usual in a BI platform deployment on the site where the user resides.
- Business Views and associated objects
  The BI platform may store Business Views, Business Elements, Data Foundations, Data Connections, and List of Values (LOVs). These objects are used to enhance the functionality of Crystal Reports.
  If these objects are first created on the destination site and then replicated to the origin site using two-way replication, they may not work properly and their data may not appear in Crystal Reports.
  It is recommended that you create the Business Views, Business Elements, Data Foundations, Data Connections, and LOVs on the origin site and then replicate them to the destination site. Make updates to the objects on the destination site or the origin site (rights permitting) and the changes will replicate back and forth properly.
- Universe overloads
  The BI platform may store universe overloads. If universe overloads are created on the destination site and then replicated to the origin site using two-way replication, they may not work properly.

To resolve this, first create the universe overloads on the origin site and replicate them to the destination site. Second, set any security on the universe overloads on the origin site and replicate them to the destination site.

- Object cleanup
  Object cleanup deletes objects that have been deleted on the other site. Object cleanup is currently only done from the origin site to the destination site.
- Federation log files
  Federation log files are written to XML files that use XML 1.1 standards. To view the log files with a browser, the browser must support XML 1.1.

Related Information

Managing object cleanup [page 905]

26.15.2 Troubleshooting error messages

This section contains error messages you may encounter in rare circumstances while using Federation. These messages will appear in the replication jobs logs or in the functionality area of a report.

1) Invalid GUID

Error example: `ERROR 2008-01-10T00:31:08.234Z The GUID ASXOOFyvy0FJnRcD0dZNTZg (found in property SI_PARENT_CUID on object number 1285) is not a valid GUID`.

This error means that you are replicating an object whose parent is not being replicated with it, and which does not already exist on the destination site. For example, an object is being replicated but not the folder that contains it. The parent object may not be replicated because the account replicating the objects does not have sufficient rights on the parent object.

2) Crystal Reports showing no data on the origin site

This error may occur if the Crystal report is using a Business View, Business Element, Data Foundation, Data Connection, or List Of Values (LOVs) that was originally created on the destination site and then replicated to the origin site.

3) Universe overloads are not applied correctly

This error may occur if the report is using a universe, which contains a universe overload that was created on the destination site and replicated to the origin site.

4) Java out of memory

Error example: `java.lang.OutOfMemoryError`.

This may occur if your Java Application Server has run out of memory while processing a replication job. Your replication job may be too big or your Java Application Server may not have enough memory.

Either increase the available memory of your Java Application Server by moving Federation Web Services to a dedicated machine, or reduce the amount of objects being replicated in one replication job.

5) Socket timeout

Error example: `Error communicating with origin site. Read timed out.`

The information being sent from the origin site to the Adaptive Job Server on the destination site is longer than the allotted timeout. Increase the socket timeout on the Adaptive Job Server, or reduce the number of objects you are replicating in your replication job.

6) Query Limit

Error example: `SDK error occurred at the destination site. Not a valid query. (FWB 00025) …...Query string is larger than query length limit.`

This error may appear if you are replicating too many objects at one time and Federation submits a query that is too large for the CMS to handle. Objects from the origin site will be committed to the destination site. However, any changes that need to be committed to the origin site will not be committed. Conflicts are resolved as specified, however manual resolution conflict flags on the object will not be set. Objects committed on the destination site will continue to work properly.

To resolve this issue, reduce the number of objects you are replicating in one replication job.

7) Replication Job Times Out

Error example: `Object could not be scheduled within the specified time interval`.

You may receive this message if your replication job times out while it waits for another replication job to finish. This may occur if you have multiple replication jobs connecting to the same origin site at the same time. The failed replication job will try to run again at its next scheduled time.

To resolve this issue, schedule the failed replication job at a time that doesn't conflict with other replication jobs that connect to the same origin site.

8) Replication Limit

Error example: `SDK error occurred at the destination site. Database access error. …. Internal Query Processor Error: The query processor ran out of stack space during query optimization. Error executing query in ExecWithDeadlockHandling.`

You may receive this message if you exceed the number of supported objects that can be replicated at one time. To resolve this issue, reduce the number of objects you are replicating in your replication job and run the job again.

9) Object dropped

Error example: `Error encountered while checking security rights`, or `Error encountered while packing object`.

This message may display if an object is dropped from the replication package. This can occur when Federation queries an object that needs replication, but before it checks for rights and the packs the object.

10) Adaptive Processing Server

Error example: `An error occurred in Job Processing Server`.

This error can occur when too many classes are loaded by Federation and there is not enough memory to process the replication job.

To resolve this issue, you need to perform both of the following steps:

1. In the command-line arguments of the Adaptive Processing Server, add the following line: `-javaArgs "XX:MaxMetaspaceSize=256m"`.

   > **Note**
   >
   > In BI 4.2 Support Package 5, you can use the MaxMetaspaceSize parameter to define metaspace memory size, as opposed to the MaxPermSize parameter.
   >
   > - If you are upgrading from versions earlier than BI 4.2 Support Package 5 to BI 4.2 Support Package 5, you need to manually edit the parameter for all existing servers.
   > - If you are performing a fresh installation of BI 4.2 Support Package 5, the parameter is replaced by default.

2. Add the following parameters to the Java Application server that you are connecting to for Federation, to reduce the size of the BIAR files that you are using:
   - `-Dbobj.biar.suggestSplit=100m`

- `-Dbobj.biar.forceSplit=100m`

11) Adjusting Adaptive Processing Servers'

A new Java argument `-XX:MetaspaceSize` is added to the APS command-line in combination with the existing `-XX:MaxMetaspaceSize` to improve the initialization experience and avoid the unwanted and full garbage collection within the Java process related to Adaptive Processing Server(s).

Testing on a VM with minimal RAM resourcing, a Default APS, and All Service included these values for MetaSpace and MaxMetaSpace appear to allow the APS to start and initialize slightly faster than the out-of-box settings. There are zero 'Full GCs' reported.

To know more about *Adjusting Adaptive Processing Servers' JAVA options to avoid Full Garbage Collection (Full GCs) with MetaSpace*, please refer the SAP Note 3001317.

12) Object Manager Space

Error example: `Could not build push package. Input/Output exception occurred: "No space left on device."`

This occurs when the temporary directory that Federation uses doesn't have enough disk space. To resolve this issue, either create extra space in the temporary directory, or use a different location for the temporary directory.

To specify a different location for the temporary directory on the origin site, add the following line to the Java Application Server's configuration files: `-Dbobj.tmp.dir=<TempDir>`.

To specify a different location for the temporary directory on the destination site, add the following line to the Adaptive Processing Server's command-line arguments: `-javaArgs "-Dbobj.tmp.dir=<TempDir>"`.

In the above examples, `<TempDir>` is the location of the temporary directory that you want to use.

13) Universe Error

Error example: `An internal error occurred while calling processDPCommands API.`

This occurs when a Universe that has been replicated has an invalid or missing Universe-to-Universe Connection relationship. To resolve this issue, run the replication job with the *Refresh from Origin* option selected, and verify that they Universe Connection is replicated.

Alternatively, you can open the Universe in Universe Designer, edit the Universe's connection, and re-commit the Universe.

Related Information

Best practices [page 920]
Current release limitations [page 923]

27 Supplementary Configurations for ERP Environments

27.1 Configurations for SAP NetWeaver integration

27.1.1 Integrating with SAP Business Warehouse (BW)

27.1.1.1 Overview

This section shows how to configure BW to enable and administer report publishing from the SAP Business Warehouse application to the BI platform.

Before beginning this section, make sure you have completed the configuration of the SAP Authentication plugin in the CMC.

Related Information

Configuring SAP authentication [page 322]

27.1.1.1.1 Setting up folders and security in the BI platform

When you define an entitlement system in the BI platform, the system creates a logical folder structure to match your SAP system. When you import roles and publish content to the BI platform, corresponding folders are created. As an administrator, you do not have to create these folders. They are created as a consequence of defining an entitlement system when configuring the SAP authentication plugin, importing roles into the CMC, and publishing content to the BI platform.

> **Note**
>
> The BI platform administrator is responsible for assigning the correct rights to these folders:
>
> - *SAP top-level folder*
>   Ensure the Everyone group has limited access to the SAP top-level folder.
> - *System ID folders*
>   Assign the principal Publisher the following rights in the CMC:
>
>   > **Note**
>   >
>   > The principal Publisher is not available until content is published.

- Add objects to folder
- View objects
- Edit objects
- Modify the rights users have to objects
- Delete objects

→ Tip

To make rights administration easier, you can create a customized Publisher access level that includes these rights, and then grant the principal Publisher this access level on relevant System ID folders.

Related Information

Working with access levels [page 129]
How rights work in BI platform [page 115]

27.1.1.1.2 Understanding the default folder security patterns

When you publish content to the BI platform from SAP, the platform automatically creates the remaining hierarchy of roles, folders, and reports. The system organizes your reports in folders that are named according to the System ID and Client Number, and according to the name of the role:

- The system creates top-level folders—that is, the SAP, 2.0, and system (`<SID>`) folders—when you define an entitlement system.
- The system creates Role folders (imported as groups into the BI platform) as necessary, when a role is published from BW.
- The system creates a Content folder for each role that content is published to.
- Security is set on each report object, so users can view only the reports that belong to their roles.

The administrator is responsible for assigning rights to members of different roles. The Content Administration Workbench is used to administer report publishing functionality from within SAP BW. You can identify roles from the SAP BW system with particular BI platform systems, publish reports, and synchronize reports between SAP BW and a BI platform deployment.

Content folders

The BI platform imports a group for each role that is added to the entitlement system as defined in the CMC.

To ensure that suitable default rights are granted to all members of a content-bearing role, grant the appropriate rights in the Content Administration Workbench for each entitlement system that is defined in the BI platform. To start the Content Administration Workbench, run transaction /CRYSTAL/RPTADMIN:

1. In the Content Administration Workbench, expand *Enterprise system* and then expand *Available systems*.
2. Double-click the system you want.
3. Click the *Layout* tab.
4. Set *Default security policy for reports* to *View*.
5. Set *Default security policy for role folders* to *View On Demand*.
6. Click *OK*.

These settings are reflected in the BI platform for all content roles. That is, roles that have content published to them. Members of these roles will now be able to view scheduled instances of reports published to other roles and will be able to refresh reports published to roles that they are a member of.

> ⓘ Note
>
> It is strongly recommended that you keep the activities of roles distinct. For example, while it is possible to publish from an administrator role, it is a better practice to publish only from publisher roles. Additionally, the function of publishing roles is only to define which users can publish content. Thus, publishing roles should not contain any content; publishers should publish to content bearing roles that are accessible to regular role members.

27.1.1.1.3 BW Events-based Scheduling

You can now schedule objects based on BW Events in the BI platform. You must establish a trusted channel of communication between an SAP NetWeaver Business Warehouse (BW) system and the BI platform to activate scheduling based on BW events.

27.1.1.1.3.1 To create and configure BW events

Context

Follow the steps below to create a BW Event:

Procedure

1. Logon to CMC.
2. Go to *Events* > *BW Events*.
3. Select to create a new event.

4. Enter the *Event Name* and *Description*.
5. Select *Create*.
   You have created a new BW event.

27.1.1.1.3.2 To add BW Events While Scheduling Report

Context

Follow the steps below to add a BW event while scheduling reports:

Procedure

1. In **CMC**, go to *Folders* and select a report.
2. In the report's context menu, choose *Schedule*.
3. In the *Navigation* pane, go to *Events* > *BW Events*.
4. Select an event from *Available Events*.
5. Add it to Events to wait for using >>.
6. In the *Navigation* pane, go to *Recurrence*.
7. Specify the parameters *Run Object*, *Number of retries allowed*, and *Retry interval in seconds*.
8. Select *Schedule*.

   Once the event is triggered, the scheduling status of the report changes to **Running** from **Pending**.

   > ⓘ Note
   >
   > The scheduling status remains in **Pending** state if any one event (s) defined under *Events to wait for* is not triggered.

27.1.1.1.3.3 To integrate BI platform and ABAP system

This topic explains how you can activate BW event-based scheduling.

Procedure

Follow the steps below:

1. Configure HTTPS/SSL for any supported application server in the BI platform and add the shared secret key at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`. See the topicConfiguring SSL in Tomcat [page 380] for Tomcat.

   > **Note**
   >
   > You can refer to SAP Product Availability Matrix (PAM) for more information on supported application servers.

2. Export the BI platform's server certificate from a browser to a local system. You can download the certificates from the Chrome browser by following the steps below.

1. Go to http://<hostname>:<port_number>/biprws. For more information on port number specific to each application, see the topic .
2. Open the developer tools of the Chrome browser by pressing F12.
3. Navigate to the *Security* tab and select *View Certificate*.
   The `Certificate` wizard is displayed.
4. In the `Certificate` wizard, go to *Details* tab and select *Copy to File*.
   The *Certificate Export Wizard* is displayed
5. Select *Next*
6. In the *Export File Format* page, choose the format *Base-64 encoded X.509 (.CER)* and select *Next*.
7. Specify a name for the certificate file and save it locally.

3. Download SAP NetWeaver BW system's certificate.

1. Launch SAP NetWeaver BW.
2. Go to transaction *STRUSTSSO2*.
3. Navigate to *System PSE* > *Subject* > *Own Certificate*.
4. Select *Download*.
5. Specify a file path and choose file format as *Base64*.
6. Select .

The SAP NetWeaver BW system's certificate is downloaded in the specified location.

4. Import the BI platform's certificate into the SAP NetWeaver BW system.

1. Go to transaction *STRUSTSSO2*.
2. Switch to *Edit* mode.
3. Select the folder *SSL client SSL Client (Standard)*.
4. Select *Import*.
5. Upload the SAP NetWeaver BW system's certificate and select *Add to Certificate List*.
   The certificate is added to the *Certificate List*.

6. Save the transaction.
5. Import the SAP NetWeaver BW system's certificate into the BI platform. Refer 12th step in the topic for more information on importing certificates.
6. Create a user in the BI platform.

> **Note**
>
> You must ensure that the user name in the BI platform should be the same as the SAP NetWeaver BW system. For example, if the SAP NetWeaver BW system name is MySystem, then you must create a user in the BI platform with the name MySystem.

7. Create an HTTP destination in SAP NetWeaver BW system.
1. Go to transaction *SM59*.
2. Select *HTTP Connections to External Server*.
3. Choose .
4. In the *RFC Destination* window, switch to the Technical Settings tab and enter the *Host*, *Port*, and *Path Prefix* as `<hostname>`, `<port_number>`, and `/biprws` respectively.
5. Switch to *Logon & Security* tab, and select *Active* against *SSL*.
6. Choose *DEFAULT SSL Client (Standard)* as the *SSL Certificate*.
7. Select *Save*.
8. Select Test Connection

for testing the connection to the HTTP destination. The connection test result appears and displays the Status Text as OK.

> **Note**
>
> The HTTP connection between SAP NetWeaver BW and the BI Platform is not be possible if the conditions mentioned below are not fulfilled.
>
> - The BW system should be updated to support TLS 1.1 and TLS 1.2 versions.
> - The BW system should support the same Cipher Suites that are supported in the BI Platform.

9. Create a process chain in SAP NetWeaver BW system.
1. Go to the transaction *RSPC*.
2. Open the context menu of *Process Chains* and choose *Create Display Component*.
3. In the *Creation of a Grouping* window, specify the *Application Component* and the *Long Description*.
   An SAP NetWeaver BW component is created.
4. In the application component's context menu, choose *Create Process Chain*.
5. Specify the Name and Description and select .
   After you specify the name of the new Process Chain, the `Insert Start Process` dialog opens. It lets you insert a Start process for the Process Chain.
6. Specify the *Process Variant*s and *Long Description*, and select .
   Maintain Start Process window appears.
7. Select *Edit Conditions* and choose *Immediate* to execute the process chain immediately.
8. Select *Save* in the `Start Time` window.
9. Select *Save* in `Maintain Start Process` window.
10. In the `Insert Start Process` window, select .
    Process Chain is created.

10. Configure the process type in the Process Chain.
1. Select the process chain created after the previous step from the column *Process Chains*.
2. Expand *Load Process and Postprocessing* folder and select *Trigger Event in SAP BOBJ BI Platform for BW Data Changes*.
   `Insert Trigger Event in SAP BOBJ BI Platform for BW Data Changes` dialog opens.
3. In the *Insert Trigger Event in SAP BOBJ BI Platform for BW Data Changes*, select .
4. Enter the *Process Variants* and *Long Description*.
5. Select .
   The `Process Maintenance` window appears.
6. Select against *Destination* to choose a destination.
7. Select against *Event* to choose an event.
8. Save the changes.
9. Select in the `Insert Trigger Event in SAP BOBJ BI Platform for BW Data Changes` dialog.
   The process type is created.
11. Activate the Process chain and execute it.

Results

The action triggers the BW Event mentioned in the process type.

27.1.1.2 Configuring the BW Publisher

The BW Publisher allows you to publish Crystal reports (.rpt files) individually or in batches from BW to the BI platform.

On Windows, you can configure the BW Publisher in one of two ways:

- Start the BW Publisher using a service on a machine hosting the BI platform. The BW Publisher service will start instances of the BW Publisher as required.
- Start the BW Publisher using a local SAP Gateway to create BW Publisher instances.

You must select the configuration method based on the requirements of your site, after considering the advantages and disadvantages of each configuration. Once you have configured the BW Publisher in the BI platform, you must configure publishing in the Content Administration Workbench.

27.1.1.3 Configuring the BW Publisher as a service

This section explains how to enable publishing of reports from BW to the BI platform using the BW Publisher as a service, perform the following procedure.

27.1.1.3.1 Distributing the BW Publisher installation

This section explains the distribution of BW Publisher service and how to separate the BW Publisher from other BI platform components.

You can load-balance publishing from BW by installing BW Publisher services on two separate machines in the same BI platform system.

When you install the BW Publisher on the machines hosting the BI platform, configure each one to use the same Program ID and SAP Gateway Host and Gateway Service. After you create an RFC destination that uses this Program ID, BW load-balances publishing between the machines hosting the BI platform. Moreover, if one BW Publisher becomes unavailable, BW continues to use the remaining BW Publisher.

You can add an additional level of system redundancy to any configuration that includes multiple BW application servers. Configure each BW application server to run an SAP Gateway. For each one, install a separate BW Publisher service on a machine hosting the BI platform. Configure each BW Publisher service to use the Gateway Host and Gateway service of a separate BW application server. In this configuration, publishing from BW can continue if either a BW Publisher or an application server fails.

If you want to separate the BW Publisher from other BI platform components, install the BW using a stand-alone SAP Gateway.

In this case you must install a local SAP Gateway on the same machine as the BW Publisher. In addition, the BW Publisher requires access to the BI platform SDK and the SAP Crystal Reports Print Engine. Thus, if you install the BW Publisher and the local SAP Gateway on a dedicated machine, you must also install the SIA Server.

27.1.1.3.2 Starting the BW Publisher: UNIX

Run the BW Publisher script to create a publisher instance or instances to handle publishing requests. It is recommended that you start one publisher instance.

Once the BW Publisher starts, it establishes a connection with the SAP Gateway Service that you specified when you ran the BI platform installation program.

27.1.1.3.3 Starting the BW Publisher: Windows

On Windows, use the Central Configuration Manager™ (CCM) to start the BW Publisher service. When you start the BW Publisher service it creates a publisher instance to service publishing requests from your BW system. If the volume of publishing requests increases, the BW Publisher automatically spawns additional publishers to meet the demand.

27.1.1.3.4 Configuring a destination for the BW Publisher service

To enable the BW Publisher, you must configure an RFC destination on your BW server to communicate with the BW Publisher service. If you have a BW cluster, configure the RFC destination on each server, using the central instance of BW as your Gateway Host in every case.

If you want to publish to multiple BI platform systems from BW, create a separate RFC destination for the BW Publisher service in each BI platform deployment. You must use unique Program IDs for each destination, but the same Gateway host and Gateway service.

27.1.1.3.5 Configuring the BW Publisher with a local SAP Gateway

> **Note**
>
> Do not use this configuration if the BI platform is installed on UNIX. Using this method on UNIX could result in unpredictable system behavior.

To enable publishing of reports from BW to the BI platform, using a local SAP Gateway, perform the following procedure:

- Installing a local SAP Gateway [page 937].
- Configuring a destination for the BW Publisher [page 938].

27.1.1.3.6 Installing a local SAP Gateway

A local SAP Gateway must be installed on the machine where you installed the BW Publisher. It is recommended that an SAP BASIS administrator perform the installation of one of these SAP Gateways.

For up-to-date instructions on installing a local SAP Gateway, see the SAP installation instructions included on your SAP Presentation CD.

For a detailed list of tested environments, consult the Product Availability Matrix (PAM) at http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540. The PAM includes specific version and Service Pack requirements for application servers, operating systems, SAP components, and so on.

After you have installed the SAP Gateway, use `regedit` to verify the `TMP` and `TEMP` registry entries under the `HKEY_CURRENT_USER\Environment` subkey. Both registry entries should hold the same string value, which must be a valid absolute directory path. If either entry's value contains the `%USERPROFILE%` variable, replace it with an absolute directory path. Typically, both registry entries are set to `C:\WINDOWS\TEMP`

27.1.1.4 Configuring a destination for the BW Publisher

To enable the BW Publisher, you must configure an RFC destination to provide BW with the location of the machine where you have installed the local SAP Gateway and the BW Publisher.

27.1.1.5 Configuring publishing in the Content Administration Workbench

The Content Administration Workbench is used to administer report publishing functionality from within SAP BW. You can identify roles from the SAP BW system with particular BI platform systems, publish reports, and synchronize reports between SAP BW and a BI platform deployment. Once you have set up SAP authentication, and have configured the BW Publisher, perform the functions outlined in this section to enable publishing. These instructions will allow you to:

- Set appropriate authorizations for different users of the Content Administration Workbench.
- Set up connections to the BI platform where content is published.
- Define which roles can publish to each BI platform.
- Publish content from BW to the BI platform.

27.1.1.6 Users who can access the Content Administration Workbench

There are three types of users who may access the Content Administration Workbench:

- Content consumers, who belong to content-bearing roles and who can view reports. They do not have authorization to do anything other than view reports.
- BI platform content publishers, who can view, publish, modify, and (optionally) delete reports from BW.
- BI platform administrators, who are able to perform all tasks within Content Administration Workbench. These tasks include defining BI platform systems, publishing reports, and performing report maintenance.

27.1.1.7 Creating roles in BW for designated content publishers

When you are configuring BW for integration with the BI platform, assess whether or not your current role structure allows you to quickly designate particular BW users as content publishers or system administrators for the BI platform systems.

It is suggested that you label any new roles you create in a descriptive manner. Examples of descriptive role names would include `BOE_CONTENT_PUBLISHERS` and `SBOP_SYSTEM_ADMINISTRATORS`.

> → Tip
>
> You can assign an administrative user either full system administration rights or a subset of those rights.

To modify the rights that these new roles (or any of your existing roles) are granted in the BI platform, you must first set up SAP Authentication and import the roles. You can then modify the rights of each imported role using the Central Management Console.

For details on creating roles, see your SAP documentation. For more information on the use of roles in administering content, see the following sections:

- Importing SAP roles [page 331].
- Setting up folders and security in the BI platform [page 929].
- Understanding the default folder security patterns [page 930].

27.1.1.8 Configuring access to the Content Administration Workbench

For each type of user that can access the Content Administration Workbench, you must apply the appropriate set of authorizations within BW. The authorizations are listed in the following tables.

Authorizations for administrative users

Authorization object	Field	Values
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Change, Display (02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Create new, Change, Display, Delete (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Create new, Delete (01, 06)

Authorization object	Field	Values
ZCNTADMRPT	ACTVT	Display, Delete, Activate, Maintain, Check (03, 06, 07, 23, 39)

Authorizations for content publishers

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Display (03)
ZCNTADMJOB	ACTVT	(New, Delete) 01, 06
ZCNTADMRPT	ACTVT	Display, Activate, Maintain, Check (03, 07, 23, 39) Delete (optional) (06) Edit (optional) (02)

Granting content publishers the right to delete reports in the BW Content Administration Workbench is optional. However, be aware that deleting a report in BW also deletes the report in the BI platform. If publishers do not have sufficient rights to delete reports in the platform, an error results.

Authorizations for content consumers

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	Execute (16)

Authorization object	Field	Values
	TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Display (03)

27.1.1.9 Defining a BI platform system

You must create a system definition within the Content Administration Workbench for each BI platform system to which you want to publish reports.

27.1.1.9.1 To add a BI platform system

Procedure

1. Execute the transaction `/crystal/rptadmin` to access the Content Administration Workbench.
2. From the *Operations* pane, select *Enterprise System*.
3. Double-click *Add new system*.
4. On the *System* tab:
   - Type a descriptive name in the *Alias* field. Avoid using spaces or special characters, as these characters need special treatment when the alias name is used while configuring Enterprise Portals.
   - Type the name of the machine that is running your CMS. If you configured your CMS to listen on a port other than the default, type **`CMSNAME:PORT`**.
   - Select *Default system* if you want to publish reports to this system from any role that has not been explicitly assigned to a BI platform system. Only one BI platform system can be the default.
     In the list of all available systems, the default system is indicated with a green checkmark.
5. Click *Save*.
6. On the *RFC Destinations* tab, add each RFC destination that is associated with this system.

   To add a destination, click the *Insert Row* button. In the list that appears, double-click the name of the RFC destination.

   > **Note**
   >
   > A BI platform system may have multiple destinations to add system redundancy. See “Distributing the BW Publisher installation”.

7. Select the check box beside the destination name you added, and click *Verify BOE definition*.

   This test verifies that BW can contact the specified BW Publisher, and can log on to this system using the Crystal entitlement user account.

8. On the *HTTP* tab:
   - In the *Protocol* field, type **`http`** or **`https`**, if the web server that is connected to the BI platform is configured for HTTPS.
   - In the *Web server host and port* field, type the fully qualified domain name or IP address of the web server that hosts BI launch pad. For an installation that uses a Java application server, include the port number. For example, type **`boserver01.businessobjects.com:8080`**.
   - In the *Path* field, type **`SAP`**
     This path is essentially the virtual path that your web server uses when referring to the `sap` subfolder of your BI platform web content. Provide an alternate value only if you have customized your web environment and the location of the platform web content files.
     Do not include a forward slash at the beginning or at the end of this entry.
   - In the *Viewer application* field, type the name of your viewer application.
     To use the default BI platform viewer that uses the Java version of BI launch pad, type **`openDocument.jsp`**
     If the BI platform was installed on Windows using the default `ASP.NET` configuration, to use the default browser, type **`report/report_view.aspx`**
9. On the *Languages* tab, select the languages of reports that will be published to this system.
10. On the *Roles* tab, add the content-bearing roles that you want to associate with this BI platform system.

    See “Importing SAP roles”.
11. Click the *Insert Row* button.

    A list of roles available to add to this system appears.

    > **Note**
    >
    > Each role can publish to only one BI platform system. If the roles you want to add to this BI platform system do not appear in the list, click *Cancel* to return to the *Roles* tab, and click *Reassign Roles*.

12. Select the roles you want to publish to this system and click *OK*.
13. On the *Layout* tab, select the default security settings for reports and roles folders published to this BI platform system.

    > **Note**
    >
    > A folder is created automatically in the BI platform for each role published to that system. The folder contains shortcuts to the reports published under that role.

    > **Note**
    >
    > Once you have configured a BI platform system, changing the default security levels here will not affect the security levels of published role folders or reports. To change the default security levels for all roles and content published to the platform, delete the roles folders and shortcuts in the system. (This will not delete the actual reports.) Change the security settings here, and republish the roles and reports.

14. Click *OK* at the bottom to save your settings and to create the BI platform system in the Content Administration Workbench.

Results

You are now able to publish reports to the BI platform from BW.

Related Information

Distributing the BW Publisher installation [page 936]
Importing SAP roles [page 331]

27.1.1.10 Publishing reports using the Content Administration Workbench

After a report has been saved to BW, you can publish it using the Content Administration Workbench. You can use the Content Administration Workbench to publish individual reports, or you can publish all reports saved to a particular role. Only a user who has the authorizations granted to a Crystal content publisher (see Creating and applying authorizations [page 957]) can use the Content Administration Workbench to publish and maintain reports.

27.1.1.11 Publishing roles or reports

1. Execute the transaction `/crystal/rptadmin` to access the Content Administration Workbench.
2. From the *Operations* pane, select *Publish reports*.
3. To find content saved to your BW system, double-click *Select reports and roles to publish*.
   A dialog box designed to help you filter the available roles and reports appears.
4. From the list, select the system or systems containing content that you want to display.

   > **Note**
   >
   > The list contains all available systems defined on the BW system.

5. Next, filter your results to limit the number of reports and roles that will be displayed. Use these options:
   - *Object version*
     Selecting "A: active" displays all reports that can be published. Selecting the blank option displays all reports. (The remaining options are SAP reserved terms.)
   - *Object status*
     Select "ACT Active, executable" to display only reports that have been published. Select "INA Inactive, not executable" to display only reports which have not been published. Leave the field blank to display all reports. (The remaining options are SAP reserved terms.)
   - *Role filter*
     If you type text in this box, only the roles that match what you type here are displayed. Use * as a wildcard character. For example, to display all roles beginning with the letter d, type "d*".

- *Report description*
  If you type text in this box, only the reports whose descriptions match what you type here are displayed. Use * as a wildcard character to match any number of characters. Use + as a wildcard to match 0 or 1 characters. For example, to display all reports whose description contains the word revenue, type *revenue*.

6. Click *OK*.
   The list of reports that meet your criteria appears in the right-hand panel.
   The reports are arranged in a hierarchy: BI platform system > Roles on that system > Reports saved to the role.
   Each item in the hierarchy is labeled with a red, yellow, or green dot. Items higher in the hierarchy reflect the status of the items that they contain, with the least favorable condition percolated to the top of the hierarchy. For example, if one report in a role is yellow (active), but all of the rest are green (published), then the role shows as yellow (active).
   - Green: The item is fully published. If the item is a BI platform system or a role, all reports in that item are published.
   - Yellow: The item is active, but not published. If the item is a report, the item is available for publishing. If the item is a role or a BI platform system, then all content is active and at least one item that the role or system contains has not been published.
   - Red: The item is SAP content, and is not available for publishing using the Content Administration Workbench. Content is not available for publishing until it has been activated using the BW Administration Workbench.
7. Select the reports that you want to publish.
   To publish all of the reports in a role, select the role. To publish all roles on a BI platform system, select the system.

   > ⓘ Note
   >
   > When you select a role (or a system), all reports contained in that role (or system) are selected. To clear this selection, clear the role (or system) check box, and then click Refresh.

8. Click *Publish*.

   > ⓘ Note
   >
   > Reports published in the background are processed as system resources become available. To use this option, click *In background* instead of *Publish*.

9. Click *Refresh* to update the display of the status of BI platform systems, roles, and reports in the Content Administration Workbench.

   > → Tip
   >
   > To view a report, right-click the report and select *View*. To see which queries are used by the report, right-click the report and select *Used Queries*.

   > ⓘ Note
   >
   > After you have published a report to the BI platform, if you want to overwrite the report you published, click *Overwrite*.

Related Information

Scheduling background publishing [page 945]

27.1.1.12 Scheduling background publishing

Publishing reports in the background, either immediately or as a scheduled job, conserves system resources. It is recommended that you publish reports in the background to improve system responsiveness.

Publishing reports periodically, as scheduled jobs, synchronizes the report information between BW and your BI platform deployment. It is recommended that you schedule all reports (or roles containing these reports). You can also manually synchronize roles and reports using the Update status option of the Report Maintenance operation. See Updating the status of reports [page 945] for details.

27.1.1.13 Updating system information for published reports

The BW Publisher uses the SAP system information entered here to update the data source of published reports. You can choose to use the local BW application server, or the central BW instance if you prefer a load balancing configuration.

27.1.1.14 Maintaining reports

Report maintenance tasks include synchronizing information about reports between the BI platform and BW (Update status), deleting unwanted reports (Delete reports), and updating reports migrated from previous versions of the platform (Post-migration).

27.1.1.14.1 Updating the status of reports

If you make a change to a published report on a BI platform system (such as changing which role a report is published to), the change is not reflected in BW until you synchronize the BI platform and BW. You can schedule a publishing job to periodically synchronize the BI platform and BW (see Scheduling background publishing [page 945]), or you can manually update the status of the report using the Report Maintenance tool.

27.1.1.14.2 Deleting reports

Deleting a published report from BW using the Content Administration Workbench also deletes the report from the BI platform. Only users who have been granted the authorizations necessary to delete reports on both BW and the BI platform system can remove reports.

> **Note**
>
> If a user has rights to delete a report on BW, but not on the BI platform system where that report is published, you may encounter an error.

27.1.1.15 Configuring the SAP http request handler

To enable viewing of reports in BW, you must configure BW to use the http request handler that is included as part of the Content Administration Workbench. Then, when a BW user opens a Crystal report from within the SAPGUI, BW can route the viewing request over the Web appropriately.

Use the transaction SICF to access the list of virtual hosts and services active on your BW system. Create a new node named `ce_url` under BW in the `default_host` hierarchy and add `/CRYSTAL/CL_BW_HTTP_HANDLER` to the handler list. You may have to manually activate this service after creating it.

27.1.1.16 Configurations for processing SAP data

27.1.1.16.1 Processing scheduled reports in SAP's batch mode

For Windows installations, you can run scheduled reports in the BI platform using SAP's batch mode.
The InfoSet and Open SQL drivers can run reports using SAP's batch or background mode when specific environment variables are set to 1. The relevant environment variables are:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (for the InfoSet driver)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE` (for the Open SQL driver)

However, it is recommended that you use this feature only when you have a distributed installation of the BI platform. When these environment variables are set to 1, the drivers run reports using SAP's batch mode, regardless of the reporting component that is actually running the report. Therefore, if you create these environment variables as system environment variables on a machine that is running a combination of BI platform servers, the drivers run all reports in batch mode (including on-demand report requests from the Crystal Reports Processing Server and the Report Application Server).

To ensure that the drivers run only your scheduled reports in batch mode (reports run by the Adaptive Job Server), avoid setting system environment variables on machines running combinations of BI platform servers. Instead, follow these steps to customize the environment variables for each Adaptive Job Server.

> **Note**
>
> SAP users who schedule reports in the BI platform may require additional authorizations in SAP.

Related Information

Scheduling a report in batch mode using an Open SQL query [page 972]

27.1.1.16.2 To process scheduled reports in SAP's batch mode

Procedure

1. Create a batch script (`.bat` file) in a text editor such as Notepad, with the following contents:

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
   %*
   ```

   This script sets the environment variables to 1 and then executes any parameters passed to the script from the command line.
2. Save the file as `jobserver_batchmode.bat` to a folder on each Adaptive Job Server machine.
3. Log on to the Central Management Console (CMC).
4. Choose *Servers*.
5. Expand the *Service Categories* node, and choose *Analysis Services*.
6. Select *Adaptive Processing Server*, and choose *Properties* in the context menu.
   The *Properties* page opens.
7. On the *Properties* page, locate the *Command line Parameters* field.

   This is the startup command for the Adaptive Job Server. For example:

   ```
   "\\SERVER01\C$\Program Files\SAO Business Objects\SAP BusinessObjects
   Enterprise\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01
   -objectType BusinessObjects Enterprise.Report -lib procReport -restart
   ```
8. Precede the default command with the full path to the `jobserver_batchmode.bat` file that you saved on the Adaptive Job Server machine.

   In this example, the batch file is saved on a machine named SERVER01 as:

   ```
   C:\Crystal Scripts\jobserver_batchmode.bat
   ```

   The new startup command for the Adaptive Job Server is:

   ```
   "\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$
   \Program Files\SAP Business Objects\SAP
   BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name
   SERVER01.report  -ns SERVER01
   -objectType BusinessObjects Enterprise.Report -lib procReport  -restart
   ```

   This new startup command launches the batch file first. The batch file in turn sets the required environment variables before executing the original startup command for the Adaptive Job Server. This ensures that the environment variables available to the Adaptive Job Server differ from the environment variables available to servers responsible for on-demand reporting (the Crystal Reports Processing Server and Report Application Server).
9. Click *Save & Close*.
10. Right-click the Adaptive Job Server and select *Start* in the context menu.

> **Note**
>
> If the Adaptive Job Server fails to start, verify your new startup command.

27.1.1.17 Configurations for SAP transports

27.1.1.17.1 Overview

The BI platform includes these transports:

- Open SQL Connectivity transport
- InfoSet Connectivity transport
- Row-level Security Definition transport
- Cluster Definition transport
- Content Administration Workbench transport
- BW Query parameter personalization transport
- MDX transport
- ODS transport

There are two different sets of the transports: Unicode compatible transports and ANSI transports. If you are running a BASIS system of 6.20 or later, use the Unicode compatible transports. If you are running a BASIS system earlier than 6.20, use the ANSI transports. All the installed transports are located in the following directory on your product distribution media: `\Collaterals\Add-Ons\SAP\Transports\`.

> **Note**
>
> When checking for possible installation conflicts, ensure that none of the object names already exists in your SAP system. Objects use a **`/crystal/`** namespace by default, so it is not necessary to create this namespace yourself. If you do create the **`/crystal/`** namespace manually, you will be prompted for license repair keys that you cannot access.

27.1.1.17.2 Configuring transports

To set up the Data Access or BW Publisher components of the BI platform , you must import the appropriate transports into your SAP system. These components use the contents of these transport files when communicating with the SAP system.

The installation and configuration procedures required on the SAP system must be performed by a BASIS expert who is familiar with the Change and Transport system and who has administrative rights to the SAP system. The exact procedure for importing transport files varies, depending upon the version of BASIS that you are running. For specific procedural details, refer to your SAP documentation.

When you first deploy the Data Access component, all users can access all of your SAP tables by default. To secure the SAP data that users can access, use the Security Definition Editor.

After you have imported transports, you must configure the appropriate levels of user access. Create the required authorizations and apply them through profiles or roles to SAP users who will be designing, running, or scheduling Crystal reports.

Related Information

Creating and applying authorizations [page 957]

27.1.1.17.2.1 Types of transports

There are two different sets of the transports: Unicode compatible transports and ANSI transports. If you are running a BASIS system of 6.20 or later, use the Unicode compatible transports. If you are running a BASIS system earlier than 6.20, use the ANSI transports. All the installed transports are located in the following directory on your product distribution: `Collaterals\Add-Ons\SAP\Transports`. The `transports.txt` file lists the Unicode compatible and ANSI transport files.

Transport types are described below:

- Open SQL Connectivity transport
  The Open SQL Connectivity transport enables the Open SQL driver to connect to and report off the SAP system.
- Row-level Security Definition transport
  This transport provides the Security Definition Editor, which is a tool that serves as a graphical interface to the /crystal/auth tables in the Open SQL Connectivity transport.
- Cluster Definition transport
  This transport provides the Cluster Definition tool. This tool enables you to build up a metadata repository for ABAP data cluster definitions. These definitions provide the Open SQL driver with the information it requires in order to report off these data clusters.

  > **Note**
  >
  > ABAP data clusters are not the same as cluster tables. Cluster tables are already defined in the DDIC.
- InfoSet Connectivity transport
  The InfoSet Connectivity transport enables the InfoSet driver to access InfoSets and SAP Queries.
- Content Administration Workbench transport
  This transport provides content administration functionality for BW systems. It is available only as a UNICODE compatible transport.
- BW Query parameter personalization transport
  This transport provides support for personalized and default parameter values in reports based on BW queries.
- BW MDX connectivity transport
  This transport enables the MDX Query driver to access BW cubes and queries. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.
- ODS connectivity transport
  This transport enables the ODS Query driver to access ODS data. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.

27.1.1.17.2.2 Checking for conflicts

The contents of the transport files are registered automatically under the SAP BusinessObjects namespace when you import the files. The SAP BusinessObjects namespace is reserved for this purpose within recent versions of R/3 and MYSAP ERP. However, object names for some objects such as authorization objects, authorization classes, and legacy objects may not contain the appropriate prefixes. It is recommended that you check these object types for conflicts prior to importing the transport files.

If the function group, any of the function modules, or any of the other objects already exists on the SAP system, then you must resolve the namespace before importing the SAP BusinessObjects transport files. Refer to your SAP NetWeaver technology platform documentation for the procedures appropriate to your version of SAP.

27.1.1.17.2.3 Importing the transport files

Read the `transports_EN.txt` file located in the following directory on your product distribution media: `\Collaterals\Add-Ons\SAP\Transports\`. This text file lists the exact names of the files that make up each transport. (The `cofiles` and `data` directories below the `transports` directory correspond to the .../`trans/cofiles` and .../`trans/data` directories on your SAP server.)

You must import the Open SQL Connectivity transport before importing the Row-level Security Definition or the Cluster Definition transports. You may import the other transports in any order.

> **Note**
>
> After copying files from CD to server, ensure that all files are writable before you import the transports. Imports fail if the import files are read-only.

> **Note**
>
> Because the transports are binary files, on UNIX installations you must add the files by FTP in Binary mode (to avoid file corruption). In addition, you must have write permissions for the UNIX server.

27.1.1.17.2.4 Transports

27.1.1.17.2.4.1 Open SQL Connectivity transport

The Open SQL Connectivity transport enables the drivers to connect to and report off the SAP system.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/OPENSQL	Function group	Open SQL functions

Object	Type	Description
/CRYSTAL/OSQL_AUTH_FORMS	Program	Helper program
/CRYSTAL/OSQL_EXECUTE	Program	Helper program
/CRYSTAL/OSQL_TYPEPOOLPROG	Program	Helper program
/CRYSTAL/OSQL_TYPEPOOLS	Program	Helper program
/CRYSTAL/OSQL_UTILS	Program	Helper program
ZSSI	Authorization object class	Reporting authorization objects
ZSEGREPORT	Authorization object	Reporting authorization object
/CRYSTAL/OSQL_CLU_ACTKEY_ENTRY	Table	Cluster metadata
/CRYSTAL/OSQL_FCN_PARAM	Table	Function metadata
/CRYSTAL/OSQL_FCN_PARAM_FIELD	Table	Function metadata
/CRYSTAL/OSQL_FIELD_ENTRY	Table	Table metadata
/CRYSTAL/OSQL_OBJECT_ENTRY	Table	Table metadata
/CRYSTAL/OSQL_RLS_CHK_ENTRY	Table	RLS metadata
/CRYSTAL/OSQL_RLS_FCN_ENTRY	Table	RLS metadata
/CRYSTAL/OSQL_RLS_VAL_ENTRY	Table	RLS metadata
ZCLUSTDATA	Table	Cluster metadata
ZCLUSTID	Table	Cluster metadata
ZCLUSTKEY	Table	Cluster metadata
ZCLUSTKEY2	Table	Cluster metadata
/CRYSTAL/AUTHCHK	Table	RLS metadata
/CRYSTAL/AUTHFCN	Table	RLS metadata
/CRYSTAL/AUTHKEY	Table	RLS metadata
/CRYSTAL/AUTHOBJ	Table	RLS metadata
/CRYSTAL/AUTHREF	Table	RLS metadata
ZSSAUTHCHK	Table	Old RLS metadata

Object	Type	Description
ZSSAUTHOBJ	Table	Old RLS metadata
ZSSAUTHKEY	Table	Old RLS metadata
ZSSAUTHREF	Table	Old RLS metadata
ZSSAUTH FCN	Table	Old RLS metadata

27.1.1.17.2.4.2 InfoSet Connectivity transport

The InfoSet Connectivity transport enables the InfoSet driver to access InfoSets. This transport is compatible with R/3 4.6c and later. Do not import this transport if you are running SAP R/3 4.6a or earlier.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/FLAT	Function group	InfoSet wrapper functions
/CRYSTAL/QUERY_BATCH	Program	Batch mode execution
/CRYSTAL/QUERY_BATCH_STREAM	Program	Streaming batch mode execution.

27.1.1.17.2.4.3 Row-level Security Definition transport

This transport provides the Security Definition Editor, which is a tool that serves as a graphical interface to the /CRYSTAL/AUTH tables in the Open SQL Connectivity transport.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/TABMNT	Function group	Function group for table maintenance view for function restrictions
/CRYSTAL/RLSDEF	Program	Main program
/CRYSTAL/RLS_INCLUDE1	Program	Include program containing the module definitions
/CRYSTAL/RLS_INCLUDE2	Program	Include program containing the subroutine definitions

Object	Type	Description
TDDAT [/CRYSTAL/AUTHFCN]	Table contents	Table maintenance definition
TVDIR [/CRYSTAL/AUTHFCN]	Table contents	Table maintenance definition
/CRYSTAL/AUTHFCNS	Definition of transport and maintenance object	Table maintenance definition
/CRYSTAL/RLS	Transaction	Main program transaction
/CRYSTAL/RLSFCN	Transaction	Helper transaction called internally by main program.

27.1.1.17.2.4.4 Cluster Definition transport

This transport provides the Cluster Definition tool. This tool enables you to build up a metadata repository for ABAP data cluster definitions. These definitions provide the Open SQL driver with the information it requires in order to report off these data clusters.

> ⓘ Note
>
> ABAP data clusters are not the same as cluster tables. Cluster tables are already defined in the DDIC.

Object	Type	Description
ZCIMPRBG	Program	Main program
ZCRBGTOP	Program	Include program
ZCDD	Transaction	Main program transaction

27.1.1.17.2.4.5 Content Administration Workbench transport

This transport provides content administration functionality for BW systems. It is available only as a Unicode compatible transport.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/CL_BW_HTTP_HANDLER	Class	Multi CE-aware HTTP request handler
/CRYSTAL/OBJECT_STATUS_DOM	Domain	Report activity

Object	Type	Description
/CRYSTAL/OBJ_POLICY_DOM	Domain	CE object security
/CRYSTAL/OBJECT_STATUS	Data element	Report activity
/CRYSTAL/OBJ_POLICY	Data element	CE object security
/CRYSTAL/CE_SYNCH	Function group	Publisher stubs
/CRYSTAL/CA_MSG	Message class	Status messages
/CRYSTAL/CE_SYNCH_FORMS	Program	Program component
/CRYSTAL/CONTENT_ADMIN	Program	Program component
/CRYSTAL/CONTENT_AD-MIN_CLASS_D	Program	Program component
/CRYSTAL/CONTENT_AD-MIN_CLASS_I	Program	Program component
/CRYSTAL/CONTENT_ADMIN_CTREE	Program	Program component
/CRYSTAL/CONTENT_ADMIN_FORMS	Program	Program component
/CRYSTAL/CONTENT_ADMIN_MOD-ULES	Program	Program component
/CRYSTAL/CONTENT_ADMIN_PAIS	Program	Program component
/CRYSTAL/CONTENT_ADMIN_PBOS	Program	Program component
/CRYSTAL/CONTENT_AD-MIN_TAB_FRM	Program	Program component
/CRYSTAL/CONTENT_ADMIN_TOP	Program	Program component
/CRYSTAL/PUBLISH_WORKER	Program	Program component
/CRYSTAL/PUBLISH_WORKER_DISP	Program	Program component
/CRYSTAL/PUBLISH_WORKER_DISP_I	Program	Program component
/CRYSTAL/PUB-LISH_WORKER_FORMS	Program	Program component
/CRYSTAL/PUBLISH_WORKER_PROC	Program	Program component
/CRYSTAL/PUB-LISH_WORKER_PROC_I	Program	Program component

Object	Type	Description
/CRYSTAL/PUB-LISH_WORKER_SCREEN	Program	Program component
/CRYSTAL/CA_DEST	Table	Application state
/CRYSTAL/CA_JOB	Table	Application state
/CRYSTAL/CA_JOB2	Table	Application state
/CRYSTAL/CA_LANG	Table	Application state
/CRYSTAL/CA_PARM	Table	Application state
/CRYSTAL/CA_ROLE	Table	Application state
/CRYSTAL/CA_SYST	Table	Application state
/CRYSTAL/MENU_TREE_ITEMS	Structure	Application state
/CRYSTAL/REPORT_ID	Table	Application state
/CRYSTAL/RPTADMIN	Transaction	Main program transaction
/CRYSTAL/EDIT_REPORT	Program	Wrapper for report edit
/CRYSTAL/EDIT_REPORT	Function Group	Functions for report edit
ZSSI	Authorization object class	Crystal Authorizations
ZCNTADMCES	Authorization object	CE operations
ZCNTADMRPT	Authorization object	Report operations
ZCNTADMJOB	Authorization object	Background job operations

27.1.1.17.2.4.6 ODS connectivity transport

This transport enables the ODS Query driver to access ODS data. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/ODS_REPORT	Function group	ODS functions

27.1.1.17.2.4.7 BW Query parameter personalization transport

This transport provides support for personalized and default parameter values in reports based on BW queries.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/PERS_VAR	Structure	Variable definition
/CRYSTAL/PERS_VALUE	Structure	Value definition
/CRYSTAL/PERS	Function Group	Personalization functions

27.1.1.17.2.4.8 BW MDX connectivity transport

This transport enables the MDX Query driver to access BW cubes and queries. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/MDX	Function group	MDX functions
/CRYSTAL/MDX_STREAM_LAYOUT	Table definition	Dataset structure
/CRYSTAL/CX_BAPI_ERROR	Class	Exception
/CRYSTAL/CX_METADATA_ERROR	Class	Exception
/CRYSTAL/CX_MISSING_STREAMINFO	Class	Exception
/CRYSTAL/CX_NO_MORE_CELLS	Class	Exception
/CRYSTAL/CX_NO_MORE_MEMBERS	Class	Exception
/CRYSTAL/CX_NO_MORE_PROPERTIES	Class	Exception
/CRYSTAL/CX_SAVE_SESSION_STATE	Class	Exception
/CRYSTAL/MDX_APPEND_DATA	Class	Dataset processor
/CRYSTAL/MDX_READER_BASE	Class	Dataset processor
/CRYSTAL/MDX_READ_DIMENSIONS	Class	Dataset processor

Object	Type	Description
/CRYSTAL/MDX_READ_MEASURES	Class	Dataset processor
/CRYSTAL/MDX_READ_PROPERTIES	Class	Dataset processor
/CRYSTAL/MDX_AXIS_LEVELS	Table type	Metadata structure
/CRYSTAL/MDX_PROPERTY_KEYS	Table type	Metadata structure
/CRYSTAL/MDX_PROPERTY_VALUES	Table type	Metadata structure
/CRYSTAL/MDX_STREAM_LAY-OUT_TAB	Table type	Metadata structure

27.1.1.18 Authorizations overview

This section provides a list of SAP authorizations that, in our experience and in our test environment, are required when carrying out common BI platform tasks in an integrated SAP environment. Additional authorization objects or fields may be required, depending upon your individual implementation.

From each authorization object, you must create an authorization and define the appropriate field values. You then apply the appropriate authorizations to the profiles (or roles) of your SAP users. The following sections describe the required authorizations and provide you with the necessary field values. For procedural details that are specific to your version of SAP, refer to your SAP documentation.

> ⓘ Note
>
> The information in this section is provided as a guideline only.

> ⓘ Note
>
> The ZSEGREPORT authorization object belongs to the ZSSI object class, which is installed when you import the SAP Integration transport files needed to support Open SQL queries.

27.1.1.18.1 Creating and applying authorizations

You must create and apply the authorizations needed by each user to access information using the Desktop Intelligence Integration for SAP. The exact procedures for creating, configuring, and applying authorizations depend upon the version of SAP that you have installed. This section provides a list of SAP authorizations that, in our experience and in our test environments, are required when carrying out common tasks when using the BI platform integrated within an SAP NetWeaver ABAP environment. Additional authorization objects or fields may be required, depending upon your individual implementation.

Related Information

Configuring publishing in the Content Administration Workbench [page 938]

27.1.1.19 Actions in BW

This section guides you through a list of various actions in BW.

27.1.1.19.1 Actions within Crystal Reports

27.1.1.19.1.1 Creating a new report from a query in a BW role

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

* **<QUERY_OWNER >** denotes the name of the owner of the query. If you specify a name, you can report off only those queries with that owner. Enter * to report off of queries with any owner.

For **<INFO_AREA>, **<INFO_CUBE>**, or **<COMP_ID >**enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.1.2 Opening an existing report from a BW role

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI. RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.1.3 Previewing or refreshing a report

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **< INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.1.4 Verifying the database (refreshing table definitions in a report)

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.1.5 Setting the location of the data source

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.1.6 Saving a report to a BW role

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

27.1.1.19.1.7 Preparing a report for translation while saving to BW

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

27.1.1.19.1.8 Saving a report and simultaneously publishing it to the BI platform

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** ***
	RSINFOCUBE	**<INFO_CUBE>** ***
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** ***
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** ***
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** **
	ACTVT	16

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

** **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

*** For **<INFO_AREA>**, **<INFO_CUBE>**, or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.1.9 Starting the BEx Query Designer™

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>**, **<INFO_CUBE>**, or **<COMP_ID>**, enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.2 Actions within BI launch pad

27.1.1.19.2.1 Logging on to the BI platform with SAP credentials

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M

27.1.1.19.2.2 Viewing an SAP BW report on demand

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>** **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.2.3 Refreshing a report from the viewer

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **

Authorization object	Field	Values
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>** **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>**, **<INFO_CUBE>**, or **<COMP_ID>**, enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.2.4 Scheduling a report

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **

Authorization object	Field	Values
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>** **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

27.1.1.19.2.5 Reading dynamic picklists in report parameters

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

27.1.1.19.3 Actions within SAP NetWeaver (ABAP)

27.1.1.19.3.1 From within Crystal Reports using the Open SQL driver

This section guides you through a list of various actions in SAP NetWeaver (ABAP) from within Crystal Reports using the Open SQL driver.

27.1.1.19.3.2 Logging onto an SAP server

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

27.1.1.19.3.3 Creating a new report

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

27.1.1.19.3.4 Opening or previewing an existing report

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

27.1.1.19.3.5 Verifying the database (refreshing table definitions in a report)

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

27.1.1.19.3.6 Setting the location of the data source

Authorization object	Field	Values
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

27.1.1.19.4 Actions within Crystal Reports using InfoSet driver and reporting off InfoSet

27.1.1.19.4.1 Logging onto an SAP server

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

27.1.1.19.4.2 Creating a new report from an InfoSet on SAP NetWeaver (ABAP)

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

> **Note**
>
> Also add enough authorizations to view data rows. For example, P_ORIG or P_APAP.

Related Information

Setting the location of the data source [page 969]

27.1.1.19.4.3 Verifying the database (refreshing table definitions in a report)

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M

27.1.1.19.4.4 Setting the location of the data source

Authorization object	Field	Values
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

27.1.1.19.5 Actions within Crystal Reports using InfoSet driver and reporting off an ABAP query

27.1.1.19.5.1 Logging onto an SAP server

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

27.1.1.19.5.2 Creating a new report from an ABAP query on SAP NetWeaver

Authorization object	Field	Values
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_TABU_DIS	ACTVT	03
	GROUP	Name of table group

27.1.1.19.5.3 Verifying the database

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

27.1.1.19.5.4 Setting the location of the data source

Authorization object	Field	Values
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Name of table group

27.1.1.19.6 Actions within the BI platform

27.1.1.19.6.1 Scheduling a report in dialog mode (with an Open SQL query)

Authorization object	Field	Values
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

> **Note**
>
> The value for CLASS is BLANK.

27.1.1.19.6.2 Scheduling a report in batch mode using an Open SQL query

Authorization object	Field	Values
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

> **Note**
>
> The value for CLASS is BLANK.

27.1.1.19.6.3 Crystal entitlement system

Authorization object	Field	Value
Authorization for file access (S_DATASET)	Activity (ACTVT)	Read, Write (33, 34)
	Physical file name (FILENAME)	* (denotes All)
	ABAP program name (PROGRAM)	*
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)

Authorization object	Field	Value
User Master Maintenance: User Groups (S_USER_GRP)	Activity (ACTVT)	Create or Generate, and Display (03)
	User group in user master maintenance (CLASS)	* **Note** For greater security, you may prefer to explicitly list the user groups whose members require access to the BI platform.

27.1.1.19.6.4 Running and designing BW BEx queries

When creating a report from a universe based on a BW BEx query, if a date dimension is included, the system administrator needs to grant `S_RS_IOBJ` authorization to both the user designing the Universe and the user running the report.

Authorization object	Field	Values
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

27.2 Configuring for PeopleSoft Enterprise integration

27.2.1 Configuring Single Sign-on (SSO) for SAP Crystal Reports and PeopleSoft Enterprise

By default, the BI platform will be configured to allow SAP Crystal Reports users to access PeopleSoft Enterprise data using Single Sign-on (SSO).

27.2.1.1 To deactivate SSO for PeopleSoft Enterprise and SAP Crystal Reports

Procedure

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select *crdb_psenterprise*.
5. Click *Remove*.
6. Click *Save & Close*.
7. On the *Servers* page in the CMC, select *Crystal Reports Services* and click *Restart server*.

27.2.1.2 To activate SSO for PeopleSoft Enterprise and SAP Crystal Reports

Context

If you have deactivated SSO for PeopleSoft Enterprise and SAP Crystal Reports and wish to reactivate it.

Procedure

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Under *Use SSO context for database logon with the following drivers*, type *crdb_psenterprise*.
5. Click *Add*.
6. Click *Save & Close*.
7. On the *Servers* page in the CMC, select *Crystal Reports Services* and click *Restart server*.

27.2.2 Configuring Secure Sockets Layer communication

You can use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your BI platform deployment.

Similar to the SSL configuration for other BI platform servers and clients, store the following key and certificate files in a secure location (under the same directory) that can be accessed by the machines in your BI platform deployment.

- The trusted certificate file (cacert.der).
- The generated server certificate file (servercert.der).
- The server key file (server.key).
- The passphrase file (passphrase.txt).

27.2.2.1 SSL configuration property file

The property file `sslconf.properties` contains all the information for required certificates and keys used by BI platform components. For example:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

The `sslconf.properties` file should be put in the folder where the BI platform is installed: `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\` by default.

27.2.2.2 To enable PeopleSoft Query Server with SSL

Prerequisites

> **Note**
>
> All values described in the following procedure are case-sensitive.

Procedure

1. Copy your SSL certificates to `C:\SSLCert`.
2. Start the Central Configuration Manager (CCM).
3. Stop the Server Intelligence Agent (SIA).
4. Double-click the SIA to open the *Properties* dialog box.
5. Click the *Protocol* tab.
6. Select *Enable SSL*.
7. For the *SSL Certificates Folder*, choose the directory containing the SSL certificates: `C:\SSLCert`.
8. For the *Server SSL Certificate File*, choose `servercert.der`.
9. For the *SSL Trusted Certificates Files*, choose `cacert.der`.

10. For the *SSL Private Key File*, choose `server.key`.
11. For the *SSL Private Key Passphrase File*, choose `passphrase.txt`.
12. Click *Apply*.
13. Start the Server Intelligence Agent.

Next Steps

You must restart your BI platform reporting servers (such as the Adaptive Job Server) before these changes will take effect.

27.2.2.3 To enable Security Bridge with SSL

Prerequisites

> ⓘ Note
>
> All values described in the following procedure are case-sensitive.

Procedure

1. Copy your SSL certificates to `C:\SSLCert`.
2. Start the Central Configuration Manager (CCM).
3. Stop the Server Intelligence Agent (SIA).
4. Double-click the SIA to open the *Properties* dialog box.
5. Click the *Protocol* tab.
6. Select *Enable SSL*.
7. For the *SSL Certificates Folder*, choose the directory containing the SSL certificates: `C:\SSLCert`.
8. For the *Server SSL Certificate File*, choose `servercert.der`.
9. For the *SSL Trusted Certificates Files*, choose `cacert.der`.
10. For the *SSL Private Key File*, choose `server.key`.
11. For the *SSL Private Key Passphrase File*, choose `passphrase.txt`.
12. Click *Apply*.
13. Start the Server Intelligence Agent.

27.2.3 Performance Tuning for PeopleSoft systems

To ensure optimal performance when you report off PeopleSoft queries, it is important to understand how queries are executed by Crystal Reports and the BI platform.

Whenever you refresh or run a report that is based on a PeopleSoft query, a connection is made to a PeopleSoft server:

- In PeopleSoft Enterprise (PeopleTools 8.46 or newer) environments, a connection is made to the *PeopleSoft Analytic Server*.
- In PeopleSoft Enterprise (PeopleTools 8.21-8.45) environments, a connection is made to the *PeopleSoft Application Server*.

27.2.3.1 Recommendations

In an optimal deployment, one or more PeopleSoft Analytic or Application Servers are set up to handle only report requests. In each of these servers, the settings for Min and Max Instances control the number of report requests that can be processed at any one time. This setup provides the following advantages:

- There is no contention between report requests and other transactional requests in the PeopleSoft server.
- It is possible to perform maintenance on the server that handles report requests without disabling the server that handles transactional requests.

In an environment where both report and transactional requests are handled by the same PeopleSoft Analytic or Application Server, you must configure the BI platform not to run more than one report at the same time. Otherwise, users will not be able to make any transactional requests if all of the PSANALYTICSRV or PSAPPSRV processes are used to run reports.

> **Note**
>
> For information on how to limit the number of scheduled report jobs and view-report-on-demand jobs, see "Managing and Configuring Servers" in the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

> **Note**
>
> It is not possible to configure the system to limit the number of Crystal Reports users who may try to access the server at the same time.

If performance issues arise, use the Psadmin configuration tool to determine if requests are being queued. As well, monitor the system resources on the PeopleSoft Analytic or Application Server machine. If virtual memory is being used because of a lack of physical memory, then processing may also slow down.

27.2.3.2 PeopleSoft servers

In a PeopleSoft Analytic Server, the process that refreshes or runs the reports is the PSANALYTICSRV process. In a PeopleSoft Application Server, the process that refreshes or runs the reports is the PSAPPSRV process.

The number of available PSANALYTICSRV or PSAPPSRV processes determines the number of reports that you can run simultaneously.

A typical PeopleSoft Analytic or Application Server configuration file contains the following information:

```
Min Instances=3
Max Instances=5
```

In this example, a minimum of three PSANALYTICSRV or PSAPPSRV processes are available at any time with the ability to increase to up to five processes. The settings do not necessarily mean that five reports can always be run at the same time; the processes may also be used to handle other tasks in the system. If no PSANALYTICSRV or PSAPPSRV processes are available to handle a request, then the request is queued until a process becomes available.

> ### Note
>
> The configuration file for PeopleSoft *Application* Servers also typically includes the `Service Timeout` parameter, which specifies how long queued requests wait for an available process. If no process becomes available within the time that is specified for the parameter, then the request times out.

28 Managing and Configuring Logs

28.1 Logging traces for components

Logs

The BI platform generates system-level messages and writes them to log files. System administrators can use these log files to monitor performance or to debug errors.

Traces

The BI platform also generates traces (recordings of events that occur during the operation of a monitored component) and collects them in log files with the `.glf` extension. Traced events range from status messages to severe exception errors. SAP support staff and developers can use traces to report on the performance of BI platform components (servers and web applications) and the activity of the monitored components.

When you set the trace log level for a component, you determine the type and verbosity of information sent to the log file. The trace log level is a filter that suppresses traces below a specified threshold. By monitoring a component trace log, you can determine whether the current instance of a component or its configuration must be changed to operate under an increased workload.

> ⓘ Note
>
> You can view BI platform log files using any text editor.

28.2 Trace log levels

The following trace log levels are available for BI platform components:

Level	Description
Unspecified	The trace log level is specified through other means (usually an `.ini` file).
None	No tracing occurs.
Low	The trace log filter allows logging error messages while ignoring warning and status messages. Important status messages are logged for component startup, shutdown,

Level	Description
	start request, and end request messages. This level is not recommended for debugging purposes.
Medium	The trace log filter is set to include error, warning, and most status messages. Least important or highly verbose status messages are filtered out. This level is not verbose enough for debugging purposes.
High	No messages are filtered. This level is recommended for debugging purposes. **⚠ Caution** This trace log level significantly affects system resources, increasing CPU usage and consuming storage space.

28.3 Configuring tracing for servers

A log message is a permanent record of events and status of a software system. Traces for a monitored BI platform deployment are written to a specific `.glf` log file and stored in the logging directory.

- On Windows, the default location is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`
- On Unix, the default location is `<INSTALLDIR>/sap_bobj/logging`

The name of the `.glf` log file includes a shorthand identifier, the server name, and a number reference, for example, `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. A new trace log file is created for the monitored server once the log file size approaches the ten-megabyte threshold. In addition, five log files are maintained at a time. As new log files are created, old log files are deleted.

You can calibrate the severity and importance of the traces collected in the log file by setting the trace log level for a specific server or group of servers.

ⓘ Note

To modify the trace log levels for specific servers or group of servers, use the Trace Log Service in the Central Management Console (CMC). To modify other parameters, manually change the trace log level and other settings in the `BO_trace.ini` file.

28.3.1 To set the log level in the CMC

Context

You can adjust the trace log level for a server without affecting other tracing settings.

Procedure

1. In the *Servers* area of the CMC, access a server.
   - Select a server from a specific category.
   - Click *Server List* in the navigation pane to access the complete list of servers, and select a server.
2. Right-click the selected server and select *Properties*.
   The *Properties* dialog box appears.
3. In the *Trace Log Service* area, select a setting from the *Log Level* list.
4. Click *Save & Close*.

Results

The new trace log level takes effect immediately.

Next Steps

To specify a different output directory for log files, include the `-loggingPath <target_directory>` parameter in the *Command Line Parameters* area. Restart the server for this setting to take effect.

Related Information

Trace log levels [page 627]

28.3.2 To set the log level for multiple servers in the CMC

Procedure

1. In the *Servers* area of the CMC, access multiple servers.
   - Select servers from a specific category.
   - Click *Server List* in the navigation pane to access the complete list of servers. Hold down `Ctrl` and click multiple servers to select them.
2. Right-click the selected servers and select *Edit Common Services*.
   The *Edit Common Services* dialog box is displayed.
3. In the *Trace Log Service* area, select a setting from the *Log Level* list.
4. Click *OK*.

Results

The new trace log level takes effect immediately.

Next Steps

To specify a different output directory for log files, include the `-loggingPath <target_directory>` parameter in the *Command Line Parameters* area. Restart the server for this setting to take effect.

Related Information

Trace log levels [page 627]

28.3.3 To configure server tracing using the BO_trace.ini file

Context

The `BO_trace.ini` file logs only errors and asserts by default.

Procedure

1. Open the `BO_trace.ini` file.
   - On Windows, the default location is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On Unix, the default location is `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. Uncomment the lines in the "Trace Syntax and Setting" section.
3. Modify the server tracing parameters. The following parameters are used for configuring server tracing:

Parameter	Default value	Possible values	Description
`sap_trace_level`	**`trace_error`**	**`trace_debug`**, **`trace_path`**, **`log_error`**,**`trace_info`**, **`trace_information`**,**`t`	Controls the minimum developer trace level that is written to the log file. **`trace_debug`** is the most verbose. **`trace_info`** and **`trace_information`** are equivalent.

Parameter	Default value	Possible values	Description
		race_error.**trace_none**	
sap_log_level	**log_error**	**log_info**,**log_information**,**log_warn**,**log_warning**,**log_error**,**log_fatal**,**log_none**	Controls the minimum administrative log level that is written to the log file. **log_info** is the most verbose. **log_info** and **log_information** are equivalent. **log_warn** and **log_warning** are equivalent.
size	**10000**KB (10 MB)	Any positive integer (KB)	Specifies the maximum size of a log file before a new **_trace.log**file is created.
keep_num	**5**	**0**, any positive integer (**N > 0**), **-1**	Determines how many trace files are retained when a new log file is created and the oldest is deleted. **-1**keeps all old log files.
administrator	**""**(empty string)	Any text string	Adds an administrator annotation to the log file. The string is inserted into the log only when display_mask & field_administrator != 0.
append	**true**	**true**, **false**	Determines whether new process instances append to existing log files (**true**) or create uniquely named log files containing the process ID (PID) and timestamp (**false**).

4. Save and close the BO_trace.ini file.

Results

The `BO_trace.ini` file is read frequently. Changes to the `BO_trace.ini` file take effect within five minutes of being saved. If you restart the CMS, changes to the `BO_trace.ini` file will take effect immediately.

Example

`BO_trace.ini` file

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

28.3.3.1 To configure tracing for a specific server

Context

The `BO_trace.ini` file specifies tracing parameters for BI platform servers. The settings affect all managed servers. Administrators can use the `BO_trace.ini` file to set particular tracing parameters for a specific server.

> ⚠ Caution
>
> New trace log level settings specified in the CMC for a specific server will overwrite any settings in `BO_trace.ini`.

Procedure

1. Open the `BO_trace.ini` file.
   - On Windows, the default location is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On Unix, the default location is `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. Use an `if` statement to specify tracing settings for a specific server. For example:

   ```
   if (process == "aps_MySIA.ProcessingServer") {
     sap_log_level=log_warning;
     sap_trace_level=trace_path;
   }
   ```

   > → Tip
   >
   > The process must be specified for the tracing setting to apply to a specific server.

3. Save and close the `BO_trace.ini` file.

Results

The modified settings will be implemented within five minutes.

28.4 Configuring tracing for web applications

Traces for a monitored BI platform deployment are written to a specific `.glf` log file and stored in a directory on the machine that hosts the web application folder.

- On Windows, the default location is `C:\Windows\System32\config\systemprofile\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\` For example, `C:\Windows\System32\config\systemprofile\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- On Unix, the default location is `$userHome/SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>/` For example, `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

The trace log level for web applications in the CMC is set to *Unspecified* by default. Trace Log settings are available for the following applications in the CMC:

- Central Management Console
- BI launch pad
- Open Document
- Web Service

> **Note**
>
> To modify the trace log levels for specific servers or group of servers, use the Trace Log Service in the Central Management Console (CMC). To modify other parameters, manually change the trace log level and other settings in the `BO_trace.ini` file. This file is deployed together with the `BOE.war` and `dswsbobje.war` files on your web application server.

Before you configure the `BO_trace.ini` file, you must use the WDeploy tool to undeploy the existing web applications from your web application server. After you configure the `BO_trace.ini` file, it must be redeployed together with the web applications on your web application server. For more information on using WDeploy to prepare, deploy, and undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

28.4.1 To set the web application trace log level in the CMC

Context

To trace other web applications, you must manually configure the corresponding `BO_trace.ini` file.

Procedure

1. In the *Applications* area of the CMC, right-click an application and select *Trace Log Settings*.

   > **Note**
   >
   > These applications have trace log settings: Fiorified BI launch pad, CMC, Open Document, Promotion Management, Version Management, Visual Difference, and Web Service.

   The *Trace Log Settings* dialog box appears.
2. Select a setting from the *Log Level* list.
3. Click *Save & Close*.
4. Restart the web application server.

Results

The new trace log level will take effect after the next web application logon.

Related Information

Trace log levels [page 627]

28.4.2 To configure tracing settings using the `BO_trace.ini` file

Context

The `BO_trace.ini` file is deployed with the `BOE` and `dswsbobje .war` files on your web application server. You can use the `BO_trace.ini` to specify tracing parameters for BI platform web applications. Because this file is not always accessible, you must undeploy the affected web application from the web application server.

Procedure

1. Use WDeploy to undeploy the web application from your web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
   - If you use the Tomcat web application server provided with the BI platform installation, you do not need to undeploy the web applications. You can modify the files directly.
     - The tracing configuration file for the `BOE.war` file is available at `<INSTALLDIR>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - The tracing configuration file for the `dswsbobje.war` file is available at `<INSTALLDIR>\Tomcat\webapps\dswsbobje\WEB-INF\conf`

   > **Note**
   >
   > If you use the bundled Tomcat web application server, skip step 2.

2. Access a predeployed version of the `BO_trace.ini` file:
   - The default location of a predeployed version of the configuration file for the `BOE.war` file is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - The default location of a predeployed version of the configuration file for the `dswsbobje.war` file is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Open the `BO_trace.ini` file.
   - On Windows, the default location is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On Unix, the default location is `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
4. Modify the server tracing parameters. The following parameters are used for configuring server tracing:

Parameter	Possible values	Description
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Determines the severity of log messages. The default log severity is **`log_error`**. Log severity follows a hierarchy, with **`log_information`** at the highest level and **`log_none`** at the lowest. When you set a log severity level, all messages of that level and lower will be displayed. For example, if you set the log severity to **`log_warning`**, messages including **`log_warning`**, **`log_error`**, and **`log_fatal`** will be written to the log file.

Parameter	Possible values	Description
		Note **log_information** and **log_warning** can be shortened to **log_info** and **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Determines the severity of trace messages. The default trace severity is **trace_error**. Trace severity follows a hierarchy, with **trace_debug** at the highest level and **trace_none** at the lowest. When you set a trace severity level, all messages of that level and lower will be displayed. For example, if you set the trace severity to **trace_path**, messages including **trace_path**, **trace_info**, and **trace_error** will be written to the log file. Note **trace_information** can be shortened to **trace_info**.

5. Save and close the `BO_trace.ini` file.
6. Use WDeploy to deploy the `.war` file on the machine that hosts the web application server.

Results

The modified tracing settings take effect after the next web application logon.

28.4.2.1 To configure tracing for a specific web application

Context

The `BO_trace.ini` file is deployed together with the `BOE` and `dswsbobje .war` files on your web application server. You can use the `BO_trace.ini` to specify tracing parameters for BI platform web applications. Because this file is not always accessible, you must undeploy the affected web application from the web application server. The following are web applications and the `.war` files associated with them:

Web application	WAR file	Predeployed location
Central Management Console	`BOE.war`	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
BI launch pad	`BOE.war`	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
Open Document	`BOE.war`	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
Web Service	`dswsbobje.war`	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

Procedure

1. Use WDeploy to undeploy the web application from your web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
   - If you use the Tomcat web application server provided with the BI platform installation, you do not need to undeploy the web applications. You can modify the file directly.
     - The tracing configuration file for the `BOE.war` file is available at `<INSTALLDIR>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - The tracing configuration file for the `dswsbobje.war` file is available at `<INSTALLDIR>\Tomcat\webapps\dswsbobje\WEB-INF\conf`

   > **Note**
   >
   > If you use the bundled Tomcat web application server, skip step 2.

2. Access a predeployed version of the `BO_trace.ini` file:
   - The default location of a predeployed version of the configuration file for the `BOE.war` file is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - The default location of a predeployed version of the configuration file for the `dswsbobje.war` file is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

3. Open the `BO_trace.ini` file.
   - On Windows, the default location is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On Unix, the default location is `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
4. Use an `if` statement to specify tracing settings for a specific web application. For example:

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

The process must be specified for the tracing setting to apply to a specific web application server. The following web applications are available after initial installation:

Web Application	Device Name
BI Launch Pad	**`WebApp_BIlaunchpad`**
Central Management Server	**`WebApp_CMC`**
OpenDocument	**`WebApp_OpenDocument`**

The following parameters are used for configuring web application server tracing:

Parameter	Possible values	Description
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Determines the severity of log messages. The default log severity is **`log_error`**. Log severity follows a hierarchy, with **`log_information`** at the highest level and **`log_none`** at the lowest. When you set a log severity level, all messages of that level and lower will be displayed. For example, if you set the log severity to **`log_warning`**, messages including **`log_warning`**, **`log_error`**, and **`log_fatal`** will be written to the log file. **Note** **`log_information`** and **`log_warning`** can be shortened to **`log_info`** and **`log_warn`**.
`sap_trace_level`	**`trace_debug`** **`trace_path`** **`trace_information`** **`trace_error`** **`trace_none`**	Determines the severity of trace messages. The default trace severity is **`trace_error`**.

Parameter	Possible values	Description
		Trace severity follows a hierarchy, with **trace_debug** at the highest level and **trace_none** at the lowest. When you set a trace severity level, all messages of that level and lower will be displayed. For example, if you set the trace severity to **trace_path**, messages including **trace_path**, **trace_info**, and **trace_error** will be written to the log file. **Note** **trace_information** can be shortened to **trace_info**.

5. Save and close the `BO_trace.ini` file.
6. Use WDeploy to deploy the `.war` file on the machine hosting the web application server.

28.5 Configuring tracing for BI platform client applications

Tracing can be activated on the following clients:

- Information design tool
- Web Intelligence Rich Client

You can configure tracing for these components by editing .ini files for each of the client types. These .ini files operate identically to the BO_trace.ini file described elsewhere in this chapter. See To configure server tracing using the BO_trace.ini file [page 982] for details on modifying the .ini file.

The files need to be located in the working directories configured for these applications (`<INSTALLDIR>\SAP BusinessObjects` by default). If they do not already exist, you may need to create them. The files have the following names:

- Information design tool: `BO_Trace.ini`
- Web Intelligence Rich Client: `WebIRichClient_trace.ini`

See the documentation for these products for more information.

28.6 Configuring extended error message tracing

For some applications, for example SAP BusinessObjects Web Intelligence, you can enable tracing to generate log files that contain extensive information about any error messages thrown by the application.

> **Note**
>
> These log files are designed to be used by SAP Support engineers. The log file format is JSON.

You enable the error message extensive information log files by modifying the following file on your SAP BusinessObjects BI installation: `extended_info.properties`.

28.7 To enable error message extensive information log files

Context

You want to retrieve extensive information about any error messages thrown by an application. To do this, you need to enable error message extensive information log files.

> **Note**
>
> In SAP BusinessObjects BI Suite version 4.2 SP5, this functionality is only supported for SAP BusinessObjects Web Intelligence.

Procedure

1. Open the following file on your SAP BusinessObjects BI installation: `extended_info.properties`.

   The default location is:
   - On Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. Set the parameters, as appropriate:

Parameter	Possible values	Description
`output.format`	• Json • none	Controls the format of the generated files. **Note** If you set the format to none, no file is generated.

Parameter	Possible values	Description
`output.size`	`<size><unit>` where `<size>` is a positive integer and `<unit>` is 'g' for gigabytes or 'm' for megabytes. **Note** The default unit is kilobytes.	The total size of all files an application can generate. When the size is exceeded, the older files are deleted.

The log files are generated in the same folder as the trace files. The default location is:

- On Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\`
- On UNIX: `<INSTALLDIR>/sap_bobj/logging/`

Files are named `<application_name>_<error_id>_exinfo.<format>`

The application name is the name of the application that threw the error. The error ID is randomly generated. The file format is the format specified in the configuration file.

Note

The only possible file extension is `.json`

A separate log file is generated for each message thrown by the specified application.

29 Integration to SAP Solution Manager

29.1 Integration overview

Supportability features have been added to the BI platform to enable integration into SAP Solution Manager. The following SAP Solution Manager™ components can be used to provide support for your BI platform deployment:

- Solution Landscape Directory
- Solution Manager Diagnostics
- Introscope by CA Wily
- SAP Passport

> **Note**
>
> To access the SAP Support Portal for SAP BusinessObjects go to: https://support.sap.com/home.html

29.2 SAP Solution Manager integration checklist

The following table summarizes what components are required to enable SAP Solution Manager to provide support for the BI platform.

SAP Solution Manager Support	Required for the BI platform
SLD registration	• SAPHOSTAGENT must be installed to enable registration of BI platform servers. **Note** The BI platform installer will automatically register servers if SAPHOSTAGENT is already installed. • Must create a connect.key file for the data supplier reporting on the back-end servers. • (Optional) For SLD registration with Apache Tomcat, SLDREG must be installed on each Tomcat server. For more information, refer to SAP Note 1508421.
SMD integration	• Must download and install SMD Agent (DIAGNOSTICS.AGENT) on all hosts of BI platform servers. • SMAdmin user account must be enabled in the BI platform.

SAP Solution Manager Support	Required for the BI platform
Performance instrumentation	• Introscope Agent must be configured to connect to Enterprise Manager. Use the BI platform installer or CMC node placeholders to configure the connections. • SMD Agent must be installed. • The BI platform must be configured to connect to the SMD Agent. Use the BI platform installer or CMC node placeholders to configure the connections.
SAP Passport	• You need to download and install SAP Passport client tool.

29.3 Managing system landscape directory registration

29.3.1 Registration of the BI platform in the System Landscape

The System Landscape Directory (SLD) is a central repository of system landscape information that is relevant for the management of the software lifecycle. The SLD contains a description of the system landscape - the systems and software components that are currently installed. SLD data suppliers register the systems on the SLD server and keep the information up-to-date. Management and business applications access the information stored in the SLD to perform tasks in a collaborative computing environment.

The System Landscape Directory-Data Supplier (SLD-DS) is the application responsible for registering the BI platform servers into the SLD server. A specific data supplier is provided for every installation of the platform to report on the following components:

- BI platform servers
- Web applications and services hosted on the WebSphere web application server.

> ⓘ Note
>
> SAP NetWeaver has a built-in SLD-DS supplier that registers the NetWeaver application server as well as hosted web applications and services. This SLD-DS is relevant for BI platform deployments that are integrated within an SAP NetWeaver environment.

The SLD-DS that reports on BI platform servers requires that the SLDREG program be installed and configured. The SLDREG program is installed when you install the SAPHOSTAGENT tool. For more information on how to access and install the SAPHOSTAGENT see the Preparation section in the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. Once SLDREG has been installed, you need to create a `connect.key` file to enable it to connect to the SLD server.

For information on how to configure the specific data supplier for WebSphere, see the *Web Application Deployment Guide*.

During the installation of the BI platform, information required for registering the BI platform is stored in a configuration file. This file contains information used by the SLD DS to connect to the BI platform database.

29.3.1.1 To create a connect.key file for the SLD data supplier

Prerequisites

Before creating a `connect.key` file for the SLD data supplier, you need to download and install the SAPHOSTAGENT. See the Preparation section in the *SAP BusinessObjects Business Intelligence Platform Installation Guide* for more details.

Context

> **Note**
>
> The `connect.key` file is required for SLD registration with the data supplier that reports on BI platform servers.

Procedure

1. Open a command line console.
2. Navigate to the default SAPHOSTAGENT install path.
   - On Windows: `Program Files\SAP\hostctrl\exe`
   - On Unix: `/usr/sap/hostctrl/exe`
3. Run the following command:
   ```
   sldreg -configure connect.key
   ```
4. Enter the following configuration details
   - User name
   - Password
   - Host
   - Port number
   - Specify to use HTTP

Results

The `sldreg` tool will create a connect.key file that will automatically be used by the data supplier to push information to the SLD server.

29.3.2 When is SLD registration triggered?

The SLD registration process is invoked by the data supplier reporting on the BI platform back-end servers in the following scenarios:

- A server node on your BI platform deployment is restarted.
- A new server or a node is added to the deployment.
- A server or a node is deleted

> **Note**
>
> If a server or a node is deleted, the SLD registration process does not modify the contents on the SLD server. To update the SLD server when a server or node is removed, delete the system from the SLD and resend it by restarting the BI platform.

The data supplier for WebSphere SLD registration can be invoked manually or set to run on a specified interval - for example, every 24 hours. For more information on configuring this data supplier refer to SAP Note 482727.

29.3.3 SLD Cleanup Before Patch Installations

Context

Data from previous versions of BI platform gets accumulated in the SLD server after a patch installation and makes it difficult to diagnose the product using SAP Solution Manager. To avoid this problem, follow the steps below on the base machine before starting any patch installation:

> **Note**
>
> The feature is available for version 4.2 SP3 and above.

Procedure

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Run the batch file bobjsldds.bat with clean parameters (`-clean`).

   > **Note**
   >
   > The system creates an xml file (with pre-defined parameters) that is pushed into the SLD server for cleanup. The cleanup refreshes after you restart SIA.

29.3.4 Logging SLD connectivity

Data supplier configuration file

A configuration file used for SLD registration is created for BI platform deployments. The file, `sldparserconfig.properties`, is located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

Logging SLD connectivity

Connectivity between the SLD server and the data supplier on the BI platform deployment is controlled through the `sldreg` tool and the `connect.key` file.

> **Note**
>
> The log file name is specified as a property in the `sldparserconfig.properties` file.

The log file for the SLD data supplier reporting on the BI platform back-end servers is by default located in the following location: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. The file is overwritten each time the data supplier is executed.

The log files for `sldreg` are by default located in the following location: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. The sldreg log file names cannot be modified, and use the following format: `sldreg_<Timestamp>.log`.

A new log file is created each time the data supplier calls sldreg.

29.3.5 Virtual Hostname

When *Server Intelligence Agent* is restarted, a data supplier file is generated for each node. The file is fed into the System Landscape Directory and later, used by SAP Solution Manager. In Business Intelligence platform 4.2 Support Package 4 and earlier, the physical hostname was added to the data supplier file. In Business Intelligence platform 4.2 Support Package 5, you can define a virtual hostname in the *sldparserconfig.properties* file to ensure that the data supplier file consumes the virtual hostname.

> **Note**
>
> By default, the data supplier file takes the physical hostname if the 'sldparserconfig.properties' file doesn't contain any virtual hostname.

Follow the steps below to add the virtual hostname in sldparserconfig.properties:

1. Go to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Edit sldparserconfig.properties file.
3. Add the following parameter: `virtualHostName = <Virtual Hostname>`.

4. Save the file.
5. Restart *Server Intelligence Agent* to ensure the changes are consumed by the data supplier file.

> **Note**
>
> The changes can be also consumed by executing the command given below:
>
> In Windows: `runbobjsldds.bat -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
>
> In Unix: `runbobjsldds.sh -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` at `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bobj-sld-ds`.

29.4 Managing Solution Management Diagnostics agents

29.4.1 Solution Manager Diagnostics (SMD) overview

The Solution Manager Diagnostics (SMD) component of SAP Solution Manager provides all functionality to centrally analyze and monitor a complete system landscape. The BI platform can be monitored by the SMD server if an SMD Agent is installed. The SMD Agent (`DIAGNOSTICS.AGENT`) gathers information for the SMD which can then be used for root cause analysis. Information collected and sent to the SMD server includes back-end server configurations and the location of server log files.

29.4.2 Working with SMD agents

The BI platform does not install the SMD Agent. The agent, `DIAGNOSTICS.AGENT`, is available to download from the following location: https://support.sap.com/swdc.

Information on installing and configuring the agent is available at: http://service.sap.com/diagnostics

Guidelines for working with the SMD Agent

The following are provided as guidelines for using SMD agents to monitor the BI platform:

- Installation order of monitored system and agent is not important. You can choose to install the SMD Agent before or after installing and deploying the BI platform.
- When installing an SMD Agent, make a note of the host name and listening port. These are critical for configuring the BI platform as a monitored system. If you have installed the agent before the monitored system, you can provide the configuration information during the BI platform installation setup. This information can also be provided later through placeholders for the nodes in the Central Management Console in your deployment.

- If the back-end servers are deployed on a distributed system, you should install an SMD Agent on every machine hosting a back-end server.
- For performance instrumentation of non-java servers, the SMD Agent is required.
- You must activate the SMAdmin user account to enable the SMD Server access the CMS.

29.4.3 SMAdmin user account

Every BI platform deployment has a user account created to facilitate SMD integration. This read-only account is used by the SMD server to log into the CMS and to gather server configuration and other information about the deployment.

The SMAdmin account is deactivated by default.

29.4.3.1 To activate the SMAdmin account

Procedure

1. In the *Users and Groups* management area of the CMC, select *User List*.
   The list of users is displayed.
2. Locate the *SMAdmin* user account.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Clear the *Account is disabled* box.
5. Click *Save & Close*.

29.5 Managing performance instrumentation

29.5.1 Performance instrumentation for the BI platform

You can use CA Wily Introscope as part of SAP Solution Manager for measuring BI platform performance instrumentation. When installing the platform, the following resources are provided for your deployment

- Introscope agent: Introscope agents collect performance metrics from BI platform Java back-end severs. Agents also collect information from the surrounding computing environment. The agents then report these metrics to the Enterprise Manager.
- The files provided to facilitate the instrumentation process. One set of files are provided for instrumentation of non-Java servers, and another set of files for instrumentation of Java servers. On the SAP Solution Manager end, the Enterprise Manager (EM) component is required. EM acts as the central repository for all Introscope performance data and metrics collected in an application environment. The EM processes performance data and makes it available to users for production monitoring and diagnosis.

29.5.2 Setting up performance instrumentation for the BI platform

There are two ways to set up performance instrumentation for workflows running on BI platform back-end servers.

1. During the installation setup for the BI platform. You will need to know the hostname and the listening port for the SMD Agent. For more information see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. If you choose this option, instrumentation will by default run once you have finished deploying the monitored system.
2. After installing the BI platform, you can provide the configuration information for the SMD agent through placeholders in the node properties in the Central Management Console (CMC).

> **Note**
>
> For instrumentation of workflows on non-Java servers, you must have the SMD Agent (`DIAGNOSTICS.AGENT`) installed.

Related Information

Working with SMD agents [page 999]

29.5.2.1 To configure nodes for instrumentation

Context

Use the following instructions if you did not provide configuration information for the SMD Agent and Enterprise Manager during installation setup for the BI platform.

Procedure

1. Go to the *Servers* area in the CMC.
2. In the navigation pane, click *Nodes*.
   All available nodes are displayed.
3. Right-click the node on which you want to perform instrumentation and select *Placeholders*.
   The Placeholders dialog box appears.
4. Modify the value for the following placeholders.

Placeholder	Description
%IntroscopeAgentEnableInstrumentation%	Enables or disables instrumentation on Java servers. Will be set to enabled if you have provided configuration details for Enterprise Manager during installation setup. Set to `true` to enable instrumentation.
%IntroscopeAgentEnterpriseManagerHost%	Host name for machine on which Enterprise Manager is installed.
%IntroscopeAgentEnterpriseManagerPort%	Listening port used by Enterprise Manager.
%IntroscopeAgentEnterpriseManagerTransport%	Communication protocol used by Enterprise Manager. Supported protocols include TCP, SSL, HTTP Tunnel, and HTTPS.
%NCSInstrumentLevelThreshold%	Used to set the level of instrumentation for non-Java servers. Set to "0" if you want to turn off instrumentation. Set to any value above "0" to activate instrumentation.
%SMDAgentHost%	The hostname of the machine on which the SMD Agent (`DIAGNOSTICS.AGENT`) is installed .
%SMDAgentPort%	The listening port used by the SMD agent.

5. Click *Save&Close*.
6. Restart the node.

Results

After the node is restarted, the new values provided will propagate to all the managed servers.

29.5.3 Performance instrumentation for the web tier

Instrumentation data for web tier components is not included with the BI platform.

29.5.4 Instrumentation log files

Once your BI platform deployment is configured to run instrumentation, messages are logged in specific locations. Checking the log files is a way to verify instrumentation status.

For instrumentation on Java back-end servers, a log file is located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs`. A separate `.log` file is created for each java process. The folder will also contain `AutoProbe.log` files that specify which methods have been loaded for instrumentation.

For instrumentation on non-Java back-end servers, log files are located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/logging/`. On Unix, the files are located in

the `<sap_bobj>\logging\` directory. Instrumentation related log files for non-Java servers are saved as `.trc` files.

For instrumentation on web application servers, a log file is located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. Two types of log files appear in this folder: `Introscope.log` and `Autoprobe.log`.

29.6 Tracing with SAP Passport

In addition to tracing BI platform components such as servers and web applications, the tracing mechanism can support the tracing of a specific action. An end-to-end trace analysis analyzes the performance of a single transaction. The consolidation of all the tracing information for a specific action enables SAP support personnel to see all the tracing data without being distracted by tracing information related to other actions.

For more information, visit 1861180.

SAP Passport

The mechanism supporting the end-to-end tracing for the BI platform is a tool called SAP Passport™. The SAP Passport client tool injects a unique identifier into all HTTP requests for a particular workflow and this identifier is forwarded to all servers used in the workflow. SAP support personnel can put together an end-to-end trace for the workflow by using this unique identifier.

> **Note**
>
> Trace log levels specified in the CMC and the `BO_trace.ini` configuration file are used if they are higher than the levels specified in the SAP Passport client tool - `SAPClientPlugin.exe`.

You can find the Passport in the logs for the back-end servers, web applications, and web services logs.

The SAP Passport client tool is not installed as part of the BI platform. To access and download the tool, go to https://support.sap.com/swdc.

30 Command Line Administration

30.1 Unix Scripts

This section details each of the administrative tools and scripts that are included with the Unix distribution of the BI platform. This section is provided primarily for reference purposes. Concepts and configuration procedures are discussed in more detail throughout this guide.

> ⓘ Note
>
> Only the user who has installed the BI Platform has the rights to execute the shell scripts in the BI Platform.

The Unix distribution of the BI platform includes a number of scripts, that together provide you with all the configuration options available in the Windows version of the Central Configuration Manager (CCM). There are a number of other scripts that provide you with Unix-specific options or serve as templates for your own scripts. Also, there are several secondary scripts that are used by the BI platform. Each script is described here and the command-line options are provided where applicable.

> ⓘ Note
>
> When entering Unix command-line parameters, you have to escape or multiply escape special shell characters. For example, if the exclamation mark "!" is used in a password, you have to escape the exclamation mark, like this: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

30.1.1 Script utilities

This section describes the administrative scripts that assist you in working with the BI platform on UNIX. The remainder of this section discusses the concepts behind each of the tasks that you can perform with these scripts. This reference section provides you with the main command-line options and their arguments.

30.1.1.1 ccm.sh

The `ccm.sh` script is installed to the `<INSTALLDIR>/sap_bobj` directory of your installation. This script provides you with a command-line version of the Central Configuration Manager. This section lists the command-line options and provides some examples.

> ⓘ Note
>
> Arguments in square brackets [ ] are optional.

> **Note**
>
> If you are unsure of a Server Intelligence Agent's name, look at the Command properties in the `ccm.config` file, and use the value that appears after the `-name` option.

> **Note**
>
> The `ccm.sh` script can only be launched by the user that performed the installation of the BI platform.

- Arguments denoted by **`<other authentication information>`** are provided in the second table.

CCM Option	Valid Arguments	Description
`-help`	*n/a*	Display command-line help.
`-start`	`all` or **`<sianame>`**	Start each Server Intelligence Agent as a process. The `all` option starts all of the nodes on the machine, including any nodes belonging to different clusters.
`-stop`	`all` or **`<sianame>`**	Stop each Server Intelligence Agent by terminating its Process ID. The `all` option starts all of the nodes on the machine, including any nodes belonging to different clusters.
`-restart`	`all` or **`<sianame >`**	Stop each Server Intelligence Agent by terminating its Process ID; then each SIA is started. The `all` option starts all of the nodes on the machine, including any nodes belonging to different clusters.
`-managedstart`	**`<fully qualified server name> <[other authentication information]>`**	Start a server.
`-managedstop`	**`<fully qualified server name> <[other authentication information]>`**	Stop a server.
`-managedrestart`	**`<fully qualified server name> <[other authentication information]>`**	Stop a server; then start the server.

CCM Option	Valid Arguments	Description
`-managedforceterminate`	**`<fully qualified server name> <[other authentication information]>`**	Stops the server immediately without completing current processing requests.
`-enable`	**`<fully qualified server name> <[other authentication information]>`**	Enable a started server so that it registers with the system and starts listening on the appropriate port. Use the fully qualified form of the server name.
`-disable`	**`<fully qualified server name> <[other authentication information]>`**	Disable a server so that it stops responding to BI platform requests but remains started as a process. Use the fully qualified form of the server name.
`-display`	**`< [other authentication information]>`**	Reports the current status of all of the servers in the cluster, including the server names, the host names, Process IDs, descriptions, whether they are running, and whether they are enabled or disabled.

The following table describes the options that make up the argument denoted by **`<[other authentication information]>`**.

> **Note**
>
> For improved security, you must always provide the credentials of an account with Enterprise authentication. Other types of authentication are not supported.

Authentication Option	Valid arguments	Description
`-cms`	**`<cmsname:port#>`**	Specify the CMS that you want to log on to. If not specified, the CCM defaults to the local machine and the default port (6400).
`-username`	**`<username>`**	Specify an account that provides administrative rights to BI platform. If not specified, the default Administrator account is attempted.

Authentication Option	Valid arguments	Description
`-password`	**`<password>`**	Specify the corresponding password. If not specified, a blank password is attempted. **Note** To specify the `-password` argument, you must also specify the `-username` argument.

The CCM reads the launch strings and other configuration values from the `ccm.config` file.

Related Information

ccm.config [page 1008]

30.1.1.1.1 Examples

These two commands start and enable all BI platform servers. The Central Management Server (CMS) is started on the local machine and the default port (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

These two commands start and enable all BI platform servers. The CCM will enable all servers in the cluster, where the CMS runs on machine MACHINE01 and port 6701:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

These two commands start and enable all BI platform servers with a specified administrative account named `SysAdmin` and the provided password:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

This single command logs on with a specified administrative account to disable an Adaptive Job Server that is running on a second machine:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

30.1.1.1.2 ccm.config

This configuration file defines the launch strings and other values that are used by the CCM when you run its commands. This file is maintained by the CCM itself, and by the other BI platform script utilities. You typically edit this file only when you need to modify a Server Intelligence Agent's command line. It is strongly recommended that you back up this file before editing it manually.

Related Information

Command lines overview [page 1014]

30.1.1.2 cmsdbsetup.sh

The `cmsdbsetup.sh` script is installed to the `<sap_bobj>` directory of your installation. The script provides a text-based program that enables you to perform the following tasks.

- Configure a CMS system database
- Reinitialize a CMS system database
- Copy data from another data source
- Change the cluster key
- Change the name of the cluster

> **Note**
>
> Before running this script, back up your current CMS system database and the contents of your Input and Output File Repositories. For more information, see the "Backing up and Restoring Your System". Also be sure to see Clustering Central Management Servers in the "Server Maintenance" chapter of the *SAP BI platform Administrator Guide* for additional information about CMS clusters and configuring the CMS database.

The script will prompt you for the name of your Server Intelligence Agent (SIA). To check the name of your SIA, view the Command properties of the SIA in the `ccm.config` file. The SIA's current name appears after the `-name` option. Or, you can use option 8 with the `serverconfig.sh` file.

Related Information

Clustering Central Management Servers [page 416]
Overview of backup and restore [page 499]

30.1.1.3 serverconfig.sh

The `serverconfig.sh` script is installed to the `<sap_bobj>` directory of your installation. This script provides a text-based program that allows you to perform the following operations.

- Add a node
- Delete a node
- Modify a node
- Move a node
- Back up server configuration
- Restore server configuration
- Modify web tier configuration
- List all nodes

30.1.1.3.1 To add/delete/modify/list nodes on UNIX

Procedure

1. Go to the `<INSTALLDIR>/sap_bobj` directory of your installation.
2. Issue the following command:

   ```
   ./serverconfig.sh
   ```

   The script prompts you with a list of options:

   1. Add a node
   2. Delete a node
   3. Modify a node
   4. Move a node
   5. Back up server configuration
   6. Restore server configuration
   7. Modify web tier configuration
   8. List all nodes
3. Type the number that corresponds to the action you want to perform.
4. If you are adding, deleting, or modifying a server, provide the script with any additional information that it requests.

30.1.2 Script templates

30.1.2.1 startservers

The `startservers` script is installed to the `<INSTALLDIR>/sap_bobj` directory of your installation. This script can be used as a template for your own scripts: it is provided as an example to show how you could set

up your own script that starts the BI platform servers by running a series of CCM commands. For details on writing CCM commands for your servers, see ccm.sh [page 1004].

30.1.2.2 stopservers

The `stopservers` script is installed to the `<INSTALLDIR>/sap_bobj` directory of your installation. This script can be used as a template for your own scripts: it is provided as an example to show how you could set up your own script that stops the BI platform servers by running a series of CCM commands. For details on writing CCM commands for your servers, see ccm.sh [page 1004].

30.1.3 Scripts used by the BI platform

These secondary scripts are often run in the background when you run the main BI platform script utilities and you do not need to run them yourself.

bobjrestart.sh

This script is run internally by the CCM to manage Server Intelligence Agent nodes. Do not run this script yourself.

env.sh

The `env.sh` script is installed to the `<sap_bobj/setup>` directory of your installation. This script sets up the BI platform environment variables that are required by some of the other scripts. BI platform scripts run env.sh as required. See the *SAP BusinessObjects Business Intelligence Platform Installation Guide* for more details.

env-locale.sh

The `env-locale.sh` script is used for converting the script language strings between different types of encoding (for example, UTF8 or EUC or Shift-JIS). This script is run by `env.sh` as needed.

initlaunch.sh

The `initlaunch.sh` script runs `env.sh` to set up the BI platform environment variables, and then runs any command that you have added as a command-line argument for the script. This script is intended primarily for use as a debugging tool by SAP BusinessObjects.

postinstall.sh

The `postinstall.sh` script is installed to the `<SCRIPTDIR>` directory of your installation. You should not run this script yourself.

setup.sh

The `setup.sh` script is installed to the root directory of your installation. This script provides a text-based program that allows you to set up your BI platform installation. This script is run automatically when you install the BI platform. It prompts you for the information that is required in order to set up the BI platform for the first time.

For complete details on responding to the setup script when you install the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*.

setupinit.sh

The `setupinit.sh` script is installed to the `</sap_bobj/init>` directory of your installation. This script copies the run control scripts to your `rc#` directories for automated startup. If you want your BI platform servers to start and stop with the machine they are installed on, run this script after the `setup.sh` script completes.

> **Note**
>
> You must have root privileges to run this script.

30.2 Windows scripts

This section details each of the administrative tools and scripts that are included with the Windows distribution of the BI platform. This section is provided primarily for reference purposes. Concepts and configuration procedures are discussed in more detail throughout this guide.

The Windows distribution of the BI platform includes the Windows version of the Central Configuration Manager (CCM). In addition to interacting with the GUI, you can choose to run the CCM executable from the command line with options to manage your servers.

30.2.1 ccm.exe

The `ccm.exe` executable is installed to the `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` directory of your installation. You can run the executable directly

from the command line to perform certain operations. This section lists the command-line options and provides some examples.

> **Note**
>
> A Server Intelligence Agent (SIA) and Central Management Server (CMS) must be running before using the command-line options of `ccm.exe` to interact with an individual server.

> **Note**
>
> Arguments in square brackets [ ] are optional.

> **Note**
>
> Arguments denoted by **`<other authentication information>`** are provided in the second table.

CCM Option	Valid Arguments	Description
`-help`	n/a	Display command-line help.
`-managedstart`	`all` or **`<fully qualified server name> <[other authentication information]>`**	Start a server.
`-managedstop`	`all` or **`<fully qualified server name> <[other authentication information]>`**	Stop a server.
`-managedrestart`	`all` or **`<fully qualified server name> <[other authentication information]>`**	Stop a server; then start the server.
`-managedforceterminate`	`all` or **`<fully qualified server name> <[other authentication information]>`**	Stops the server immediately without completing current processing requests.
`-enable`	`all` or **`<fully qualified server name> <[other authentication information]>`**	Enable a started server so that it registers with the system and starts listening on the appropriate port.

CCM Option	Valid Arguments	Description
`-disable`	`all` or **`<fully qualified server name> <[other authentication information]>`**	Disable a server so that it stops responding to BI platform requests but remains started as a process.
`-display`	**`< [other authentication information]>`**	Reports the current status of all of the servers in the cluster, including the server names, the host names, Process IDs, descriptions, whether they are running, and whether they are enabled or disabled.

The following table describes the options that make up the argument denoted by **`<[other authentication information]>`**.

> **Note**
>
> You must always provide the credentials of an account with Enterprise authentication.

Authentication Option	Valid arguments	Description
`-cms`	**`<cmsname:port#>`**	Specify the CMS that you want to log on to. If not specified, the CCM defaults to the local machine and the default port (6400).
`-username`	**`<username>`**	Specify an account that provides administrative rights to the BI platform. If not specified, the default Administrator account is attempted.
`-password`	**`<password>`**	Specify the corresponding password. If not specified, a blank password is attempted. **Note** To specify the `-password` argument, you must also specify the `-username` argument.
`-authentication`	**`<authentication type>`**	Specify the authentication type. Only **`secEnterprise`** is supported.

The CCM reads the launch strings and other configuration values from the `ccm.config` file.

30.2.1.1 Examples

The following examples assume that a Server Intelligence Agent (SIA) and Central Management Server (CMS) are started and running. Before using the command-line options of `ccm.exe` to interact with an individual server, you can use the following Windows command to start the SIA service:

```
net start "Server Intelligence Agent (NODENAME)"
```

The SIA can also be stopped using `net stop "Server Intelligence Agent (NODENAME)"`.

This command starts all BI platform servers:

```
ccm.exe -managedstart all
```

This command starts an Adaptive Job Server. The CMS was started on port 6701, rather than on the default port:

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

This command enables an Adaptive Job Server with a specified administrative account named `SysAdmin`:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

This command logs on with a specified administrative account to disable an Adaptive Job Server that is running on a second machine:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

30.3 Server Command Lines

30.3.1 Command lines overview

This section lists the command-line options that control the behavior of each BI platform server.

When you start or configure a server through the Central Management Console (CMC) the server is started (or restarted) with a default command line that includes a typical set of options and values. In the majority of cases, you need not modify the default command lines directly. Moreover, you can manipulate the most common settings through the various server configuration screens in the CMC. For reference, this section provides a full listing of the command-line options supported by each server. You can modify each server's command line directly if you need to further customize the behavior of the BI platform.

Throughout this section, values provided in square brackets [ ] are optional.

> **Note**
>
> The following tables list the supported command-line options. BI platform servers use a number of internal options that are not listed in these tables. These internal options must not be modified.

30.3.1.1 To view or modify a server's command line

Procedure

1. Use the Central Management Console (CMC) to stop the server.
2. Right-click the server and select *Properties*.
3. On the *Properties* screen, modify the command line for the server, and click *Save & Close*.
4. Start the server.

30.3.2 Standard options for all servers

These command-line options apply to all of the BI platform servers, unless otherwise indicated. See the remainder of this section for options specific to each type of server.

Option	Valid Arguments	Behavior
`-requestPort`	`<port>`	Specify the port that the server listens on. The server registers this port with the CMS. If unspecified, the server chooses any free port greater than 1024. **Note** This port is used for different purposes by different servers. Before changing, see the section on changing the default server port numbers in the *BI platform Administrator Guide*.
`-loggingPath`	`<absolute path>`	Specify the path where log files are created.

30.3.2.1 UNIX signal handling

On UNIX, the BI platform daemons handle the following signals:

- `SIGTERM` results in a graceful server shutdown (exit code = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE`, and `SIGILL` result in a rapid shutdown (exit code = 1).

30.3.3 Central Management Server

This section provides the command-line options that are specific to the CMS. The default path to the server on Windows is `<INSTALLDIR>\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

The default path to the server on UNIX is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_cmsd`.

Option	Valid Arguments	Behavior
`-threads`	**`<number>`**	Specifies the number of working threads that the CMS initializes and uses. The value can be between 12 and 150, and is set to 50 by default.
`-reinitializedb`		Cause the CMS to delete the system database and recreate it with only the default system objects. All existing data in the database is lost when it is recreated.
`-quit`		Force the CMS to quit after processing the `-reinitializedb` option.
`-receiverPool`	**`<number>`**	Specify the number of threads the CMS creates to receive client requests. A client may be another SAP BusinessObjects server, the Report Publishing Wizard, Crystal Reports, or a custom client application that you have created. The default value is 5. Normally you will not need to increase this value, unless you create a custom application with many clients.
`-maxobjectsincache`	**`<number>`**	Specify the maximum number of objects that the CMS stores in its memory cache. Increasing the number of objects reduces the number of database calls required and greatly improves CMS performance. However, placing too many objects in memory may result in the CMS having too little memory remaining to process queries. The default value is 100000.

Option	Valid Arguments	Behavior
`-ndbqthreads`	**`<number>`**	Specify the number of CMS worker threads sending requests to the database. Each thread has a connection to the database, so you must be careful not to exceed your database capacity. In most cases, the maximum value you should set is 20.
`-oobthreads`	**`<number>`**	If your cluster includes more than eight CMS cluster members, ensure that the command-line for each CMS includes this option. Specify the number of CMS services in your cluster. This option ensures that the cluster can sustain heavy load.

Related Information

Standard options for all servers [page 1015]

30.3.4 Crystal Reports Processing Server and Crystal Reports Cache Server

The Crystal Reports Processing Server and the Crystal Reports Cache Server are controlled in much the same way from the command line. The command-line options determine whether the server starts as a Processing Server, a Cache Server, or both. Options that apply only to one server type are noted below.

The default paths to the servers on Windows are:

- `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0 \win64_x64\cacheserver.exe`.
- `<INSTALLDIR>\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe`.

The default paths to the servers on UNIX are:

- `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_cachesd`.
- `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_procd`.

Option	Valid Arguments	Behavior
`-cache`		Enable Cache Server functionality.

Option	Valid Arguments	Behavior
`-deleteCache`		Delete the cache directory every time the server starts and stops.
`-report_ProcessExtPath`	**`<absolutepath>`**	Specify the default directory for processing extensions.

Related Information

Standard options for all servers [page 1015]

30.3.5 Job Servers

This section provides the command-line options that are specific to Adaptive Job Servers.

The default path to the server on Windows is `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`.

The default path to the server on UNIX is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_jobsd`.

Option	Valid Arguments	Behavior
`-dir`	**`<absolutepath>`**	Specify the data directory for the Job Server.
`-maxJobs`	**`<number>`**	Set the maximum number of concurrent jobs that the server will handle. The default is five.
`-requestJSChildPorts`	**`<lowerbound-upperbound>`**	Specify the range of ports that child processes should use in a firewall environment. For example, `6800-6805` limits child processes to six ports. **Note** For this option to take effect, you must also specify the `-requestPort` setting.

Option	Valid Arguments	Behavior
`-report_ProcessExtPath`	**`<absolutepath>`**	Specify the default directory for processing extensions. For details, see the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

Related Information

Standard options for all servers [page 1015]

30.3.6 Adaptive Processing Server

The Adaptive Processing Server uses parameters defined for the SAP Java Virtual Machine (SAP JVM). Refer to SAP JVM documentation for more information.

30.3.7 Report Application Server

This section provides the command-line options that are specific to the Report Application Server.

The default path to the server on Windows is `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

The default path to the server on UNIX is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras/boe_crystalrasd`.

Option	Valid Arguments	Behavior
`-ipport`	**`<port>`**	Specify the port number for receiving TCP/IP requests when running in standalone mode (outside of the BI platform).
`-report_ProcessExtPath`	**`<absolutepath>`**	Specify the default directory for processing extensions. For details, see the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

Option	Valid Arguments	Behavior
`-ProcessAffinityMask`	`<mask>`	Use a mask to specify exactly which CPUs that RAS will use when it runs on a multi-processor machine. The mask is in the format `0xffffffff`, where each `f` represents a processor, and the list of processors reads from right to left (that is, the last `f` represents the first processor). For each `f`, substitute either 0 (use of CPU not permitted) or `1` (use of CPU is permitted). For example, if you run the RAS on a 4 processor machine and want it to use the 3rd and 4th processors, use the mask `0x1100`. To use the 2nd and 3rd processors, use `0x0110`. **Note** RAS uses the first permitted processors in the string, up to the maximum specified by your license. If you have a two processor license, `0x1110` has the same effect as `0x0110`. **Note** The default value of the mask is `-1`, which has the same meaning as `0x1111`.

Related Information

Standard options for all servers [page 1015]

30.3.8 Web Intelligence Processing Server

This section provides the command-line options that are specific to the Web Intelligence Processing Server.

The default path to the server on Windows is `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

The default path to the server on UNIX is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/WIReportServer`.

Option	Valid Arguments	Behavior
`-ConnectionTimeoutMinutes`	**`<minutes>`**	Specify the number of minutes before the server will timeout.
`-MaxConnections`	**`<number>`**	Specify the maximum number of simultaneous connections that the server allows at one time.
`-DocExpressEnable`		Enables caching of Web Intelligence documents when the document is being viewed.
`-DocExpressRealTimeCachingEnable`		Enables real time caching of Web Intelligence documents.
`-DocExpressCacheDurationMinutes`	**`<minutes>`**	Specify the amount of time (in minutes) that content is stored in cache.
`-DocExpressMaxCacheSizeKB`	**`<kilobytes>`**	Specify the size of the document cache.
`-EnableListOfValuesCache`		Enables the caching per user sessions of lists of values
`-ListOfValuesBatchSize`	**`<number>`**	Specify the maximum number of values that can be returned per list of values batch.
`-UniverseMaxCacheSize`	**`<number>`**	Specify the number of universes to be cached.
`-WIDMaxCacheSize`	**`<number>`**	Specify the maximum number of Web Intelligence documents that can be stored in cache.

Related Information

Standard options for all servers [page 1015]

30.3.9 Input and Output File Repository Servers

This section provides the command-line options that are specific to the Input and Output File Repository Servers.

The default path to the servers on Windows is `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

The default path to the program that provides both servers on UNIX is: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_filesd`. By default, the Server Intelligence Agent will launch one instance of `boe_filesd` for the Input File Repository Server and one instance for the Output File Repository Server.

Option	Valid Arguments	Behavior
`-rootDir`	**`<absolutepath>`**	Set the root directory for the various subfolders and files that are managed by the server. File paths used to refer to files in the File Repository Server are interpreted relative to this root directory. **Note** All Input File Repository Servers must share the same root directory, and all Output File Repository Servers must share the same root directory (otherwise there is a risk of having inconsistent instances). Additionally, the input root directory must not be the same as the output root directory. It is recommended that you replicate the root directories using a RAID array or an alternative hardware solution.

Option	Valid Arguments	Behavior
`-tempDir`	**`<absolutepath>`**	Set the location of the temporary directory that the FRS uses to transfer files. Use this command line option if you want to control the location of the FRS temporary directory, or if the default temporary directory name generated by the FRS exceeds the file system path limit (which will prevent the FRS from starting). **Note** Do not specify an existing directory for this option. The specified directory will be emptied when the FRS starts, and removed when the FRS shuts down. If you use an existing directory, it will be emptied and removed.
`-maxidle`	**`<minutes>`**	Specify the number of minutes after which an idle session is cleaned up.
`-legacymode`		Allow older versions of the SDK, or clients older than the 4.0 release, to fully access the BI platform.
`-vsaFileLoc`	**`<absolutepath>`**	Set the absolute path to the virus scan adapter library file. **Note** All Input File Repository Servers must share the same root directory, and all Output File Repository Servers must share the same root directory (otherwise there is a risk of having inconsistent instances).

Related Information

Standard options for all servers [page 1015]

30.3.10 Event Server

This section provides the command-line options that are specific to the Event Server.

The default path to the server on Windows is `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`.

The default path to the server on Unix is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_eventsd`.

Option	Valid arguments	Behavior
`-cleanup`	**`<minutes>`**	Specify the frequency (in minutes) with which the server cleans up listener proxies. The value represents the amount of time it takes to perform two cleanups. For example, if you specify a value of 10, the proxies will be cleaned up every five minutes.

Related Information

Standard options for all servers [page 1015]

31 Repository Diagnostic Tool

31.1 Overview of the Repository Diagnostic Tool

The Repository Diagnostic Tool (RDT) is a command-line tool that scans, diagnoses, and repairs inconsistencies that may occur between your Central Management Server (CMS) system database and the File Repository Server (FRS) filestore, or inconsistencies that can occur in the metadata of InfoObjects stored in the CMS database.

During normal operations, it is unusual for the CMS system database to have inconsistencies. However, inconsistencies may occur during unexpected events such as disaster recovery, back-up restoration, or network outages. During these events, the CMS system database may be interrupted while performing a task. This can cause inconsistencies with objects in the CMS system database.

The RDT scans the CMS system database and identifies inconsistencies in such objects as reports, users, user groups, folders, servers, universes, universe connections, and other objects.

The RDT scans for three types of inconsistencies.

- Object to file inconsistencies.
  These are inconsistencies that can occur between InfoObjects in the CMS database and the corresponding files in the File Repositories. For example, a file that is stored in the FRS may be missing a corresponding object in the CMS system database.
- InfoObject metadata inconsistencies.
  These are inconsistencies that may exist in an InfoObject's object definition (metadata) in the CMS database. For example, an InfoObject may reference another InfoObject that does not exist in the CMS database.
- Relationship inconsistencies.
  There inconsistencies occur when a relationship exists between two InfoObjects but one of them has been deleted. Only relations EnterpriseNode-Server, Service-Server, ServiceContainer-Server are processed.

The RDT performs two functions, depending on the parameters that you provide when you run the tool:

- It scans the CMS system database and FRS filestore, reports inconsistencies, and outputs a log file in XML format with suggested actions to repair the inconsistencies.
- It scans and repairs the inconsistencies identified in the CMS system database and FRS, and outputs the actions taken to a log file in XML format.

31.2 Using the Repository Diagnostic Tool

Context

The Repository Diagnostic Tool (RDT) is available on any machine with a Central Configuration Manager (CCM) installed on it. This command-line tool scans, diagnoses, and repairs inconsistencies that may occur between

the Central Management Server (CMS) system database and the File Repository Server (FRS) filestore, or inconsistencies that may occur in an InfoObject's metadata.

It is recommended that you back up your CMS database and FRS filestore, and run the RDT against the backed-up version while your BI platform services are down. If this is not possible, the RDT can be run on an active database.

If you want to run the RDT on an active database, keep the following considerations in mind:

- The RDT will use one database connection while it runs.
- The RDT will only check the consistency of the database to the point in time where it started running. Any inconsistencies that occur while the RDT is running will not be logged or fixed.
- It is recommended that the host machine running the RDT have memory above the normal system recommendations available for processing RDT transactions:
  - A database of 50,000 InfoObjects or fewer should have an additional 350 MB available for processing
  - A database of 50,000 to 400,000 InfoObjects should have an additional 1.7 GB available for processing
  - A database of 400,000 to 1,000,000 InfoObjects should have an additional 4 GB available for processing
- The RDT does not have to be run from your CMS server. Running it on a separate machine can help reduce any impact on system performance.
- The tool may have a moderate impact on database performance while being run.

The RDT does not require the CMS service to be running; the RDT runs directly against the CMS database.

31.2.1 To use the Repository Diagnostic Tool

Procedure

1. If you are running the tool on a Windows computer, open a command window and run the following command.

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe <arguments>`, where `<arguments>` is the list of parameters that you want to specify.
2. If you are running the tool on a Unix computer, open a /usr/bin/sh compatible shell, and run the following command.

   `.<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>`
   where `<platform>` is “linux64_x64” and `<arguments>` is the list of parameters that you want to specify.

   > **Note**
   >
   > When entering Unix command-line parameters, you may need to escape or multiply escape special shell characters. For example, if the exclamation mark “!” is used in a password, you may need to escape the exclamation mark, like this: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

Results

The Repository Diagnostic Tool scans your repository for inconsistencies. Depending on the parameters that you specify, it either diagnoses and logs inconsistencies, or it repairs inconsistencies and logs the action that it takes.

`Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` lists the inconsistencies that the tool finds. If you had the tool repair the discrepancies that it finds, it also creates the file `Repo_Repair_yyyy_mm_dd_hh_mm_ss.xml`. This file details which objects are repaired and any orphaned files that were deleted. If there are inconsistencies that could not be repaired these will also be listed.

The path to the log files can be specified by the `outputdir` parameter. If this parameter is not specified, the default directory for the log files is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` on Windows, and `./sap_bobj/enterprise_xi40/reposcan` on Unix.

> **Note**
>
> The application also provides a default XSL file that is used with the XML file to produce an HTML page. The XSL file is stored in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` on Windows, and `./sap_bobj/enterprise_xi40/reposcan` on Unix

For a list of the warning messages and recommended actions that the RDT takes when it finds inconsistencies, see *Inconsistencies in the CMS metadata* and *Inconsistencies between the CMS and the FRS* .

Related Information

Inconsistencies in the CMS metadata [page 1036]
Inconsistencies between the CMS and the FRS [page 1035]

31.2.2 Repository Diagnostic Tool Parameters

The RDT accepts the parameters in the following table:

> **Note**
>
> Command-line arguments override any parameter file entries while executing.

> **Note**
>
> For SAP HANA database parameter options, see SAP Note 1916845.

General Parameters

Parameter	Optional or Mandatory	Description
`dbdriver`	Mandatory	The type of driver used to connect to the CMS database. Accepted values are: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `sqlanywheredatabasesubsystem`
`connect`	Mandatory	The connection details that are used to connect to the CMS database. For example: `-connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"`

Parameter	Optional or Mandatory	Description
`dbkey`	Mandatory	Enter the cluster key for your BI platform deployment. If you do not know the cluster key, reset the cluster key by following these steps: **Note** If the machine is in a cluster, these steps will have to be done for all cluster members. Back up the CMS database and filestore before proceeding. 1. Launch the Central Configuration Manager (CCM). 2. In the CCM, right-click the Server Intelligence Agent (SIA) and choose *Stop*. Do not proceed to Step 3 until the SIA status is "Stopped". 3. Right-click the SIA and choose *Properties*. 4. On the Configuration tab, click *Change* next to *CMS Cluster Key Configuration*. 5. A warning message is displayed. Click Yes to continue. 6. In the *Change Cluster Key* dialog box, enter the same eight-character key in both the *New Cluster Key* and *Confirm New Cluster Key* fields. **Note** The RDT will not run if the `dbkey` parameter is omitted, or if the cluster key is incorrect. **Note** The cluster key displayed in the CCM is encrypted, and cannot be used in the `dbkey` parameter. For more information on cluster keys see "Securing the BI Platform" in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
`inputfrsdir`	Mandatory	The file path of the Input File Repository Server. **Note** The user account you are logged on with is used to execute the command-line tool. It must have full control to the file location.

Parameter	Optional or Mandatory	Description
`outputfrsdir`	Mandatory	The file path of the Output File Repository Server. **Note** The user account you are logged on with is used to execute the command-line tool. It must have full control to the file location.
`outputdir`	Optional	The file path where the RDT writes the log files. The default value is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` on Windows, and `./sap_bobj/enterprise_xi40/reposcan` on Unix.
`count`	Optional	The number of approximate errors to scan. This helps ensure optimum performance. The upper count is 2e31 - 1. A value of 0 is interpreted as the entire repository. The default value is 1000.
`repair`	Optional	Tells the RDT to repair all inconsistencies it may find. The default behavior is to only report inconsistencies but not to perform any repairs. If the `-repair` parameter exists on the command line, the RDT reports and repairs all inconsistencies. **Caution** This process will delete any orphaned objects or files in the repository database.
`scanfrs`	Optional	Specifies whether the RDT scans the CMS and FRS for inconsistencies.
`scancms`	Optional	Specifies whether the RDT scans the CMS for inconsistencies between InfoObjects.
`submitterid`	Optional	Specifies the User ID to replace missing or invalid IDs for scheduled objects. If no value is provided, the RDT does not replace the invalid IDs. If the provided User ID doesn't exist in the CMS, the RDT prompts for a valid ID. This parameter is only used when the RDT operates in repair mode.

Parameter	Optional or Mandatory	Description
`startid`	Optional	Specifies the object in the CMS database to start the scan for. For example, if you've already scanned the first 500 objects in your repository, you can set **`-startid=501`** to start a new scan at the 501st object. The default value is **`1`**.
`optionsfile`	Optional	Specifies the file path to a parameter file. The parameter file is a text file that lists each command-line option and its values. The file should have one parameter per line. **Note** With this option, you can set all parameters in a Text file as described above. Use this option to point to the parameter file without entering the parameters on the command-line.
`syscopy`	Optional	This parameter is used when you copy the repository database. You must run the tool on the newly created copy, which will update the copy to prevent it from clustering with the source system servers. If the copy will not be able to communicate with the source system, this is not necessary. It should only be used with the mandatory parameters and not be combined with other optional parameters in this list. **Note** Be careful not to run the RDT with the `syscopy` parameter on your source system.
`trace`	Optional	This parameter generates traces (recordings of events that occur during the operation of a monitored component) and collects them in log files with the .glf extension at the location: `<SAP_BOBJ_INST_DIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging`

Parameter	Optional or Mandatory	Description
`scankind`	Optional	Enter the infoobject kind that you want to scan for inconsistencies. **Example** SI_KIND - Web Intelligence reports, Crystal reports List of supported infoobjacts that can be scanned for inconsistencies include: • folder • crystalreport • shortcut • user • usergroup • calendar • connection • category • objectpackage • publication • pdf • rtf • txt • note • word • excel • tenant • profile • program • agnostic • universe • hyperlink • fullclient • powerpoint • scopebatch • metadata.dataconnection • webi • qaaws • lcmjob • overload • xcelsius

Parameter	Optional or Mandatory	Description
		• biwidgets • mon.probe • liveoffice • mdanalysis • visualdiff • ao.workbook • dsl.metadatafile • afdashboardpage • ao.presentation • ccis.dataconnection • platformsearchqueue • metadata.businessview • platformsearchindex • platformsearchcontentstore • platformsearchcontentsurrogate **Note** The output xml of scankind displays the list of inconsistencies with respect to infoobjects. In other words, the affected file objects are not be listed.
scandays	Optional	Enter the number of days for which you want RepoScan to check for inconsistencies. **Example** Any real number other than 0. **Note** This option works based on the current system time.

Relationship are not scanned during partial scans. Partial scans occur if one of the three following options is used:

- startid
- scankind
- scandays

Inconsistencies in the relationships

Warning message	Inconsistency	Suggestion	Action
`Relation '<Name>' from object ID <ID> has an invalid target (Object ID = <ID>)`	The edge of a relation does not exist anymore.	Allow the application to remove the relationship.	Deleted relationship.

The following parameters are used if the Repository Diagnostic Tool is running on an active clustered CMS.

Using the RDT against a clustered CMS

Parameter	Optional or Mandatory	Description
`requestport`	Optional	The port number that the RDT uses to communicate to the CMS. Accepts whole, positive numbers. By default, the tool uses the value from the operating system of the machine that the RDT is running on.
`numericip`	Optional	Whether the RDT uses the numeric IP address instead of the hostname for communication between the CMS and the machine that the RDT is running on. Acceptable values are **`True`** and **`False`**. The default value is **`False`**.
`ipv6`	Optional	The ipv6 name of the machine that the RDT is running on. Accepts a string. The default value is the hostname of the machine that the RDT is running on.
`port`	Optional	The ipv4 name of the machine that the RDT is running on. Accepts a string. The default value is the hostname of the machine that the RDT is running on.
`threads`	Optional	The number of threads to use. Accepts whole, positive numbers. The default value is **`12`**.

The following parameters are used when the RDT uses SSL to communicate with the CMS database that it scans.

Using the RDT with SSL

Parameter	Optional or Mandatory	Description
`protocol`	Optional	Specifies whether the tool should run in SSL mode. The only accepted value is **`ssl`**.

Parameter	Optional or Mandatory	Description
ssl_certdir	Optional	The directory that contains the SSL certificates.
ssl_trustedcertificate	Optional	The file name of the certificate.
ssl_mycertificate	Optional	The file name of the signed certificate.
ssl_mykey	Optional	The file name of the file that contains the private SSL key.
ssl_mykey_passphrase	Optional	The file name of the file that contains SSL passphrase.

Example

The following Windows example scans the CMS and FRS for both kinds of inconsistencies, and repairs the inconsistencies that it finds.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect “UID=root;PWD=<Password1>;DSN=<myDsn>;HOSTNAME=<myHostname>;PORT=<3306>”
-inputfrsdir “C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Input”
-outputfrsdir    “C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Output”
-dbkey <cluster key>
-repair
```

Example

Unix example:

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

31.3 Inconsistencies between the CMS and the FRS

The following table describes the inconsistencies that may exist between a Central Management Server (CMS) database and the File Repository Servers (FRS) that are recognized by the Repository Diagnostic Tool (RDT).

- Warning Message
  The warning message that is written to the scan and repair log files.

- Inconsistency
  An explanation of the inconsistency that the RDT finds for the object.
- Suggestion
  The action that the RDT suggests when it finds an inconsistency. This is found in the scan log file.
- Action
  The action that the RDT takes to repair an inconsistency. This is found in the repair log file.

Warning Message	Inconsistency	Suggestion	Action
<Object Name> object <Object Type> (Object ID = <ID>) is referencing files that do not exist in the FRS (<File Name>).	The object exists in the CMS database, but there is no corresponding file in the FRS.	Allow the application to delete this object. Any objects that are descendants of this object will also be deleted.	Deleted this object from the repository.
File <File Name> exists in the Input or Output FRS, but there is no corresponding InfoObject in the repository.	The file exists in the FRS, but there is no corresponding file in the CMS database.	Allow the application to remove the unlinked file.	No action taken.
<Object Type> Object <Object Name> (Object ID = <ID>) has file <File Name>. The stored file size is <Size> bytes which does not match the actual file size <Size> bytes.	The size of the file does not match the InfoObject file size.	Allow the application to update the object with the correct file size.	Updated the object to have the correct file size.
This directory contains no files.	The FRS folder is empty.	Allow the application to remove the directory.	Removed the empty folder.

31.4 Inconsistencies in the CMS metadata

The following table describes the inconsistencies that can occur in the metadata of the objects that are in a Central Management Server (CMS) system database, that are recognized by the Repository Diagnostic Tool (RDT).

- Warning Message
  The warning message that is written to the scan and repair log files.
- Inconsistency
  An explanation of the inconsistency that the RDT finds for the object.
- Suggestion
  The action that the RDT suggests when it finds an inconsistency. This is found in the scan log file.
- Action
  The action that the RDT takes to repair an inconsistency. This is found in the repair log file.

Warning Message	Inconsistency	Suggestion	Action
<Object Type> Object <Object Name> (Object ID = <ID>)'s parent object is	The object has a missing or invalid Parent Object ID.	Allow the application to move the object to the "BOE Repair" folder.	Moved the object and its children objects to the BOE Repair folder.

Warning Message	Inconsistency	Suggestion	Action
missing (Parent Object ID = <ID>).			
<Object Type> Object <Object Name> (Object ID = <ID>) owner object is missing (Owner Object ID = <ID>).	The object has a missing or invalid Owner Object ID.	Allow the application to assign the object to the Administrator.	Assigned the object to the Administrator.
<Object Type> Object <Object Name> (Object ID = <ID>) submitter object is missing (Submitter Object ID = <ID>).	The object has a missing or invalid Submitter Object ID.	The recommendation that the RDT displays depends on whether you've provided a value for the `-submitterid` parameter. • If you provide this parameter, the recommendation is "Allow the application to update the object with the provided submitter ID". • If you don't provide this parameter, the recommendation is "Reschedule the object or use the -submitterid command line to replace the invalid submitter ID."	If you provide a value for the `-submitterid` parameter, the RDT applies the value for the object's submitter ID. If you don't provide a value for this parameter, the RDT takes no action. When you reschedule the object, the CMS applies a new ID.
<Object Type> Object '<Object Name>' (Object ID = <ID>) property of last successful instance refers to a missing object (Last Successful Instance Object ID = <ID>).	The object's last successful instance is missing or invalid.	Allow the application to recalculate the property.	Recalculated the property.
<Object Type> Object '<Object Name>' (Object ID = <ID>)'s calendar object is missing (Calendar Object ID = <ID>).	The object references a calendar that doesn't exist.	Reschedule the object with an existing calendar. No action can be taken by this application.	No action taken.
<Object Type> Object '<Object Name>' (Object ID = <ID>)'s required scheduling server group is missing (Server Group Object ID = <ID>).	The preferred server does not exist.	Reschedule the object and choose an existing server group. No action can be taken by this application.	No action taken.

Warning Message	Inconsistency	Suggestion	Action
<Object Type> Object '<Object Name>' (Object ID = <ID>)'s list of pending events contains missing object(s) (Event Object ID(s) = <ID>).	The event or events that this object is waiting on does not exist.	Reschedule the object to wait for existing event objects. No action can be taken by this application.	No action taken.
<Object Type> Object '<Object Name>' (Object ID = <ID>)'s list of events to trigger contains missing object(s) (Event Object ID(s) = <ID>).	This object triggers an event that does not exist.	Allow the application to remove missing events from the object's list of events to trigger.	Removed the missing events from the object's list of events to trigger.
<Object Type> Object '<Object Name>' (Object ID = <ID>)'s Access Control list references a missing principal (Principal Object ID = <ID>).	Orphaned Access Control entry.	Allow the application to remove the missing principal from the object's Access Control list.	Removed the missing principal from the object's Access Control list.
<Object Type> Object '<Object Name>' (Object ID = <ID>)'s Access Control list references a missing access level (Access Level Object ID = <ID>).	Orphaned Access Control entry.	Allow the application to remove the missing access level from the object's Access Control list.	Removed the missing access level from the object's Access Control list.
<Object Type> Object <Object Name> (Object ID = <ID>) has multiple Favorites folders.	A specific user account has multiple favorites folders.	Allow the application to consolidate multiple folders into a single Favorites folder.	All Favorites folders have been consolidated into a single Favorites folder.
<Object Type> Object <Object Name> (Object ID = <ID>) contains invalid Input File entries (<Files>).	The object contains invalid entries in its Input Files list.	Allow the tool to remove the object's invalid entries from its Input Files list.	Removed the invalid entries from the object's Input Files list.
<Object Type> Object <Object Name> (Object ID = <ID>) contains invalid Output File entries (<Files>).	The object contains invalid entries in its Output Files list.	Allow the tool to remove the object's invalid entries from its Output Files list.	Removed the invalid entries from the object's Output Files list.
<Object Type> Object <Object Name> (Object ID = <ID>)'s required caching server group is missing (Server Group Object ID = <ID>).	The object is missing the required caching server group.	Reschedule the object and choose an existing server group.	No action taken.
<Object Type> Object <Object Name> (Object ID = <ID>)'s required processing server group is missing (Server Group Object ID = <ID>).	The object is missing the required processing server group.	Reschedule the object and choose an existing server group.	No action taken.

Warning Message	Inconsistency	Suggestion	Action
<Object Type> Object <Object Name> (Object ID = <ID>)'s list of profiles contains missing object(s) (Profile Object ID(s) = <ID>).	The object contains missing objects in its list of profiles.	Please update your Publication with existing profiles. No action can be taken by the application.	No action taken.

31.5 Managing Restful SDK inside BOE WebApp

To activate the BIPRWS WebApp part of the BOE Webapp in 4.3 SP03, set the flag to *true* in the below location:

```
<BOE_INST_DIR>\SAP BusinessObjects\tomcat\webapps\BOE\WEB-
INF\internal\Global.properties
```

Set `use.boe.internal.biprws=true`

When the flag is set to true, the internal applications do not depend on Restful application URL or the relative path flag set in CMC.

The feature is advantageous as it helps avoid the following:

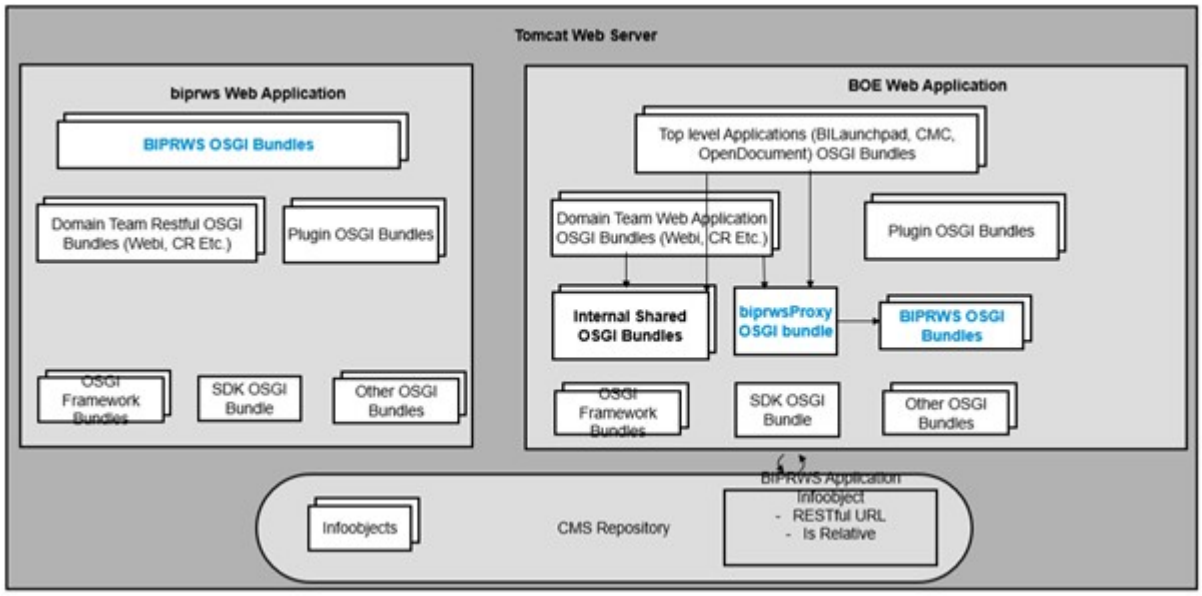
- CORS (Cross-Origin Resource Sharing) issues
- Internal and external system connectivity issues
- Pinging BOE WebApp to keep session alive
- Proxy related issues as there is no separate configuration for BIPRWS and BOE.
- Web application cluster related issues.

The existing deployment with BOE Webapp works seamlessly after upgrade.

Logging:

Once BIPRWS is merged into BOE Web App, the logs are generated as part of the BI Launch pad or CMC application log's location.

Architecture:



32 HTTP Strict Transport Security (HSTS)

32.1 Configuring HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) is a policy mechanism to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking.

It allows web servers to declare that web browsers (or other complying user agents) should automatically interact with it using only HTTPS connections. This provides Transport Layer Security (TLS/SSL), unlike the insecure HTTP usage.

HSTS is an IETF standards track protocol and is specified in RFC 6797.

The HSTS Policy is communicated by the server to the user agent via an HTTP response header field named "Strict-Transport-Security".

1. This policy specifies a period during which the user agent should only access the server in a secure fashion.
2. Websites using HSTS often do not accept clear text HTTP, either by rejecting connections over HTTP or systematically redirecting users to HTTPS (though this is not required by the specification).
   This is to make sure that a user-agent not capable of doing TLS might not be able to connect to the site.
3. The protection only applies after a user has visited the site at least once relying on the principle of Trust on first use.

How it works

When a user enters or selects a URL to the site that specifies HTTP, the URL automatically upgrades to HTTPS without making an HTTP request. This prevents the HTTP man-in-the-middle attack from occurring.

In 4.3 SP03, SAP BOE supports the HSTS arrangement.

Before Configuring HSTS, your application server should be configured with SSL.

To enable HSTS Support, perform the steps given below:

1. Stop Tomcat.
2. Navigate to `E:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\default`.
3. Open Global.properties file and set below parameters.
   1. `hsts.enabled` True/False. Default value set to false.
   2. `hsts.Include.SubDomains` True /False - It effects all subdomains of the domain name.
   3. `hsts.MaxAge.Seconds` = 31536000.
   4. Default = 365days.
4. Save the changes.

33 Rights Appendix

33.1 About the rights appendix

This rights appendix lists and describes most rights that can be set on different objects in the BI platform system. In cases where you require more than one right to perform a task on an object, it also provides information about the additional rights that you require and which objects you must have those rights on. For more information about setting rights see the *Setting Rights* chapter in the *SAP BI platform Administrator Guide*.

33.2 General rights

The rights in this section apply to multiple object types. Many of these rights also have equivalent owner rights. Owner rights are rights that apply only to the owner of the object on which the rights are being checked.

The following rights apply only to objects that can be scheduled:

- The *Schedule the document to run* right.
- The *Schedule on behalf of other users* right.
- The *Schedule to destinations* right.
- The *View document instances* right.
- The *Delete instances* right.
- The *Pause and resume document instances* right.
- The *Reschedule instances* right.

Right	Description
View objects	Lets you view objects and their properties. If you do not have this right on an object, the object is hidden in the BI platform system. This right is a basic right that is required for all tasks.
Add objects to the folder	Lets you add objects to a folder. This right also applies to objects that behave like folders such as inboxes, `Favorites` folders, or object packages.
Edit objects	Lets you edit object content and the properties for objects and folders.
Modify the rights users have to objects	Lets you modify security settings for an object.

Right	Description
Securely modify the rights users have to objects	Lets you grant rights or access levels that you already have on an object to other users. To do this, you require this right on the user and the object itself. For more information about this right, see the "Setting Rights" chapter of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
Define server groups to process jobs	Lets you specify which server group to use when objects are processed. This right only applies to objects for which you can specify processing servers. To specify a server group, you also require the *Edit objects* right on the object.
Delete objects	Lets you delete objects and their instances.
Copy objects to another folder	Lets you create copies of objects in other folders in the CMS. To do this, you also require the *Add objects to the folder* right on the destination folder. **Note** When an object is copied, the explicit security on the object is not copied; the new object inherits security settings from the destination folder, but you must reset explicit security.
Replicate content	Lets you replicate objects to another system in a federated deployment.
Schedule the document to run	Lets you schedule objects.
Schedule on behalf of other users	Lets you schedule objects for other users or groups. The user or group that you schedule the object for becomes the owner of the object instance. To schedule an object for other users or groups, you also require the following rights: • This right on the user or group. • The *Schedule the document to run* right on the object.
Schedule to destinations	*Schedule to destinations* is the parent right of *Schedule to FTP, SMTP, BI Inbox, SFTP*, and *File System*. You should select *Schedule to destinations* right in combination with the specific child right to schedule an object to the specific destination. For example, you should select the rights *Schedule to destinations* and *Schedule to FTP* to schedule an object to an FTP destination. If you are updating the BI landscape from BI 4.2 SP04 or earlier to BI 4.2 SP05 or

Right	Description
	later, then refer to 2675734, 2642221, 2626550 for more information on troubleshooting. To schedule an object to destinations, you also require the following rights: • The *Schedule the document to run* right on the object that you want to schedule • The *Add objects to the folder* right on the recipient inbox (if you want to schedule to an inbox destination) • The *Copy objects to another folder* right on the object that you want to schedule (if you want to send a copy to an inbox destination instead of a shortcut) **Note** If *Schedule to destination* right is assigned through *Access Level* such as *Full Control* or *Schedule* roles in BI 4.2 SP04 or earlier, then after the update to BI 4.2 SP05 Patch 03 or later, the child destination rights such as *Schedule to FTP, SMTP, SFTP, BI Inbox*, and *File System* are also granted. For *Access Levels* such as *View on Demand* and existing *Custom* roles in BI 4.2 SP04 or earlier, then after the update to BI 4.2 SP05 Patch 03 or later, the child destination rights are not granted by default. You should grant the rights manually. Therefore, the recurrence schedule job created in BI 4.2 SP04 or earlier will schedule objects successfully in BI 4.2 SP05 Patch 03 or later.
Schedule to FTP	Allows you to schedule an object to an FTP destination.
Schedule to SFTP	Allows you to schedule an object to an SFTP destination.
Schedule to SMTP	Allows you to schedule an object to an SMTP destination.
Schedule to File System	Allows you to schedule an object to a File System destination.
Schedule to BI Inbox	Allows you to schedule an object to a BI Inbox destination.
View document instances	Lets you view object instances. This right is a basic right that is required for all tasks that you perform on object instances.
Delete instances	Lets you delete object instances only. If you have the *Delete objects* right, you do not require this right to delete instances.
Pause and resume document instances	Lets you pause or resume object instances that are running.
Reschedule instances	Lets you reschedule object instances.

Right	Description
Add comments -BI Commentary	Lets a user add comments to a document using BI Commentary.
Delete comments -BI Commentary	Lets a user delete comments from a document using BI Commentary.
Delete comments that the user created -BI Commentary	Lets a user delete comments that he created from a document using BI Commentary.
Modify comments -BI Commentary	Lets a user modify comments in a document using BI Commentary.
Modify comments that the user created -BI Commentary	Lets a user modify comments that he created in a document using BI Commentary.
View Comments - BI Commentary	Lets a user view comments on a document using BI Commentary.
View Comments that the user created - BI Commentary	Lets a user view comments that he created in a document using BI Commentary.
Hide Comments - BI Commentary	Lets a user hide comments on a document using BI Commentary.
Hide Comments that the user created - BI Commentary	Lets a user hide comments that he created on a document using BI Commentary.
Bulk Add comments - BI Commentary	Allows a user to migrate the comments along with the document.

33.2.1 Destination Rights

Each Destination is associated with a specific destination right. The BOE admin should ensure that the users have the desired destination rights.

Earlier, when a user had a *Schedule to Destinations* right, he could schedule to all available destinations. From SP05 release onwards, individual destination rights were given to users where *Schedule to Destinations* correspond only to *Default Enterprise Location*.

New rights are introduced under General Rights for each destination:

- Schedule to File System
- Schedule to FTP
- Schedule to Inbox
- Schedule to SFTP
- Schedule to SMTP
- Schedule to Google Drive

For more information on *General Rights*, refer to General rights [page 1042].

To provide these destination options while scheduling, the Administrator has to grant respective individual destination rights. Refer 2621878. If the user has a right only on *Schedule to Destinations*, he will not be able to schedule to the destination FTP, Inbox, SFTP, SMTP, and Files System.

If *Schedule to Destinations* right is assigned at an earlier version through Access level, such as Full Control or Schedule roles, after an upgrade to 4.2 SP05, additional (newly Introduced) rights are also granted. Thus, schedule to any destination succeeds.

If it is assigned through *View On Demand* access level, any Custom role, or directly assigned (individual right, not by any role), then only Schedule to *Default Enterprise Location* pass, and other destinations fail.

For more information, please refer to and

33.3 Rights for specific object types

33.3.1 Folder rights

To make rights administration easier, it is recommended that you set rights on folders so that their contents inherit security settings. Folder rights include the following:

- General rights that apply to the folder object.
- Type-specific rights that are intended for the folder's contents (such as the *Print the report's data* right on Crystal reports).

33.3.2 Categories

The rights in this section are general rights that have a specific meaning in the context of public and personal categories.

> **Note**
>
> Objects in categories do not inherit rights that are set on the categories.

Right	Description
Add objects to the folder	Lets you create new categories within categories. This right is not needed to add objects to a category.
Edit objects	Lets you do the following: • Modify category properties. • Move the category into another category as a sub-category. • Add objects to the category. • Remove objects from the category. To move a category into another category as a sub-category, you also require the following rights: • The *Delete objects* right on the original category. • The *Add objects to the folder* right on the destination category.
Delete objects	Lets you delete the category.

33.3.3 Crystal reports

The rights in this section apply to Crystal reports only.

> **Note**
>
> These rights only apply when Crystal reports are in the BI platform environment. When you download Crystal reports to your local disk, these rights are ineffective. To prevent this, you can deny the *Download files associated with the object* right on the Crystal report.

Right	Description
Print the report's data	Lets you print the report.
Refresh the report's data	Lets you refresh report data.
Export the report's data	Lets you export report data to any format when you view the report online in the Crystal Reports viewer. To export report data in RPT format, you also require the *Download files associated with the object* right.
Download the files associated with the object	This right lets you do the following: • Export the report in RPT format. • Open the report in Crystal Reports Designer. • Schedule the report in RPT format to external destinations.

33.3.4 Web Intelligence documents

The rights in this section apply to Web Intelligence documents only.

Right	Description
Use Lists of Values	Lets you use lists of values.
Export the report's data	Allows a user to export reports' data to Text, CSV, Excel, PDF or HTML format. This command also allows to use the Print command that generates a PDF file you can print.
Query script - enable viewing (SQL , MDX...)	Lets you view query scripts (SQL and MDX).
Query script - enable editing (SQL , MDX...)	Lets you edit query scripts (SQL and MDX). You can also edit Free-hand SQL (FHSQL) data sources.
Refresh the report's data	Lets you refresh document data.
Edit Query	Lets you edit queries in the document.
Refresh List of Values	Lets you refresh lists of values for prompts when you create the prompt or when you view the document. To do this, you also require the *Use Lists of Values* right on the document.
Send to	Lets you send documents to the Scheduler, to a BI platform Inbox, or to send as hyperlinks in email. This right also lets Web Intelligence Rich Client users send documents as email attachments.

33.3.5 Users and groups

You can set rights on users and groups as you would on other objects in the BI platform environment. The rights in this section are type-specific rights that apply to user and group objects only or general rights that have a specific meaning in the context of users and groups.

> **Note**
>
> Users and subgroups can inherit rights from group membership.

> **Note**
>
> The creator of a user account is considered as the owner of the account. However, after the user account is created, this user, for whom the account is created is also considered as owner.

Right	Description
Edit objects	Lets you do the following:

Right	Description
	• Edit properties for the user or group. • Manage group membership. To add a user or group to another group, you require this right on the user or group and on the destination group.
Change user password	Lets you do the following: • Change the password for your user account. To do this, you also require the *Edit objects* right on your user account. • Change the password for another user's account. To do this, you also require the *Edit objects* right and the *Modify the rights users have to objects* right on the user account. **Note** This right does not affect the following user password settings: *Password never expires* *User must change password at next logon* *User cannot change password* **Note** This right does not apply to data source credentials for SAP BusinessObjects Universes.
Subscribe to publications	Lets you add the user to publications as a recipient.
Schedule on behalf of other users	Lets you schedule objects on behalf of the user so that the user becomes the owner of the object instance. To do this, you also require the *Schedule on behalf of other users* right on the object.
Add or edit user attributes	Lets you change the value of a user's email address or custom user attributes. This right is applicable to users.
Add or edit user attributes (owner right)	Lets the owner of a user object change the value of the user's email address or custom user attributes. This right is applicable to users.
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no Preferences menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or

Right	Description
	millimeters) to use in reports in the Web Intelligence or BI launch pad application.

33.3.6 Access levels

The rights in this section apply to access levels only.

Right	Description
Use access level for security assignment	Lets you assign the access level when you add principals to access control lists for objects. To do this, you also require the *Modify the rights users have to objects* right or the *Securely modify the rights users have to objects* right on the principal and the object. In cases where the *Securely modify the rights users have to objects* right is granted, you must also have the same access level granted to yourself on the object.

33.3.7 Universe (.unx) rights

The rights in this section apply to universes created with the information design tool, or .unx universes. The rights listed are type-specific rights that apply to universes only, or general rights that have a specific meaning in the context of universes.

> **Note**
>
> Universe rights apply only to universes published to a repository. These rights do not apply when the universe is saved to a local folder.

Right	Description
View objects	Lets you access and view the universe.
Edit objects	Lets you to republish the universe.
Delete objects	Lets you delete the universe.
Retrieve universe	Lets you to retrieve a published universe and edit the underlying resources (business layer and data foundation) in the information design tool.

Right	Description
	Note You must also have the information design tool application right *Retrieve universes* granted.
Edit security profiles	Lets you to insert, edit, and delete security profiles for the universe in the information design tool security editor. **Note** This right is not required to view security profiles or to change security profile aggregation options.
Assign security profiles	Lets you to assign and unassign security profiles to users and groups in the information design tool security editor.
Data Access	Lets you retrieve data from the universe and refresh documents based on the universe. In the information design tool, this right lets you to preview the result set in the query panel.
Create and edit queries based on this universe	Lets you create and edit queries that are based on the universe. In the information design tool, this right lets you open the query panel and run a query on the universe.
Save for all users	Lets you save the universe for all users. **Note** You must also have the information design tool application right *Save for all users* granted.

33.3.8 Universe object-access levels

When designers create a business layer using the information design tool, they assign an object-access level to every object in the universe. The object-access levels are:

Public (default)
Controlled
Restricted
Confidential
Private

Once the universe is published in the repository, you can grant access to universe objects based on the object-access levels assigned in the application. For example, you can grant Public access to the Everyone group. This allows users in the Everyone group to see the objects in the universe designated as Public.

Each object-access level grants more access to objects than the previous one. Public is the lowest level. Principals granted Public access can only see objects designated as Public. Principals granted Controlled access can see objects designated as Public and Controlled. Private is the highest level setting and grants principals access to all object-access levels, in other words, all objects in the universe.

> **Note**
>
> Object-access level security settings override any security settings that the universe inherits.

> **Note**
>
> For .unx universes, object-access level security settings are taken into consideration with the object security defined by the security profile. For more information on security profiles, see the *Information Design Tool User Guide*.

Related Information

Assigning universe object-access levels [page 1052]

33.3.8.1 Assigning universe object-access levels

Prerequisites

To set universe object-access level security, you require the *Modify the rights users have to objects* right on the universe.

Procedure

1. In the *Universes* area of the CMS, select the universe.
2. Click *Action* > *Universe Security*.
3. In the *Universe Security* dialog box, for the user or group, select the object-access level in the *Object Level Security* list.

33.3.9 Connection rights

The rights in this section are type-specific rights that apply to universe connections or general rights that have a specific meaning in the context of universe connections. These rights apply to connections published in the repository.

Relational connection rights

Right	Description
View objects	Lets you view the connection.
Edit objects	Lets you edit the connection parameters.
Download connection locally	Lets you use universes created on the connection in Web Intelligence Rich Client in offline mode. Lets you use the local middleware driver in the information design tool. To do so, select the local middleware option in the information design tool preferences, otherwise queries to the database will use the server middleware. This right is also needed to edit a secured connection in the information design tool.
Delete objects	Lets you delete the connection.
Copy objects to another folder	Lets you copy the connection from one folder to another.
Data Access	Lets you retrieve content from the database specified in the connection. In the information design tool, this right lets you browse table data from the connection and data foundation editors. It also lets you preview the result set in the query panel.
Use connection for Stored Procedures	Lets you use the stored procedures in the database specified for the universe connection.
Use connection for Free-Hand SQL scripts	Lets you run SQL scripts on the connection.

OLAP connection rights

Right	Description
View objects	Lets you view the connection.

Right	Description
Edit objects	Lets you edit the connection parameters in the information design tool connection editor.
Delete objects	Lets you delete the connection.
Copy objects to another folder	Lets you copy the connection from one folder to another.
Download connection locally	Lets you use universes created on the connection in Web Intelligence Rich Client in offline mode.

33.3.10 Applications

33.3.10.1 CMC

Right	Description
Log on to the CMC and view this object in the CMC	Enables a user to log on to the CMC
Allow access to Instance Manager	Enables a user to access the Instance Manager
Allow access to Relationship Query	Enables a user to run relationship queries in the CMC
Allow access to Security Query	Enables a user to run security queries in the CMC

33.3.10.2 Fiorified BI launch pad

Right	Description
Logon to new Fiorified BI launch pad	Enables a user to logon to the fiorified BI launch pad.
Organize	Enables a user to move and copy objects, add objects to the `Favorites` folder, and create shortcuts to objects
Send to Business Objects inbox	Enables a user to send objects to recipient BI Inboxes
Send to email destination	Enables a user to send objects to recipients via email
Send to file location	Enables a user to send objects to a file location
Send to FTP location	Enables a user to send objects to an FTP location

Right	Description
Send to SFTP location	Enables a user to send objects to an SFTP location. SFTP destination has similar properties as the FTP destination page with an additional fingerprint option which has to be provided by the user. Every SFTP server has fingerprint option in properties. Matching/validation of the fingerprint is done in the backend by CMS.

33.3.10.3 BI workspaces

Right	Description
Create and edit BI workspaces	Enables a user to create new BI workspaces and to edit existing BI workspaces
Create and edit modules	Enables a user to create new modules and to edit existing modules
Edit BI workspaces	Enables a user to edit existing BI workspaces (but does not enable a user to create new workspaces)
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

33.3.10.4 Web Intelligence

The access rights in this section apply to the Web Intelligence application, including the Rich Client, and can affect viewers and query panels in the application.

Right	Description
Data: Enable data tracking	Enables a user to track changed data.
Data: Enable formatting of changed data	Enables a user to select formatting for changed data.
General: Enable Desktop client access	Enables a user to use Web Intelligence Desktop (Rich Client).
Desktop: Export documents	In Web Intelligence Rich Client, enables a user to export documents to the BI Platform repository.

Right	Description
Desktop: Save documents for all users	In Web Intelligence Rich Client, enables a user to save documents locally without any security.
Documents: Disable automatic refresh on open	Prevents documents from automatically refreshing when they are opened.
Documents: Enable auto-save	Enables documents to be automatically saved, if autosaving is activated in the CMC by the administrator.
Documents: Enable creation	Enables a user to create new documents.
General: Edit Web Intelligence preferences	Enables a users to changes Web Intelligence preferences in the BI Launch Pad.
General: Enable Web client access	Enables a user to use the Web Intelligence web client.
Query: Edit script generated from universe	In the query panel, enables a user to edit the SQL or MDX query scripts generated from universe.
Query: Edit Free-Hand SQL	Enables a user to edit Free-Hand SQL query scripts.
Query: View script generated from universe	In the query panel, enables a user to view the SQL or MDX query scripts generated from universe.
Query: View Free-Hand SQL	Enables a user to view Free-Hand SQL query scripts.
Reporting: Create and edit breaks	Enables a user to create and to edit breaks.
Reporting: Create and edit conditional formatting rules	Enables a user to create and to edit conditional formatting rules.
Reporting: Create and edit predefined calculations	Enables a user to create and to edit predefined calculations.
Reporting: Create and edit input controls and groups	Enables a user to create and to edit input controls.
Reporting: Create and edit filters and consume input controls	Enables a user to create and edit report filters and also allows them to consume the input controls.
Reporting: Create and edit sorts and rankings	Enables a user to create and to edit sorts and rankings.
Reporting: Create formulas, variables, groups and references	Enables a user to create formulas, variables, groups and references.
Reporting: Enable document change	Enables a user to edit report formatting. Without this access right, the Design mode isn't available.
Reporting: Merge objects	Enables a user to synchronize data using merged dimensions in reports and in the data manager.
Reporting: Insert and remove reports, tables, charts and cells	• Enables a user to insert and to remove reports, tables, charts, and cells. • Enables the duplicates workflow (copy/paste).

33.3.10.5 Information design tool

Right	Description
Administer security profiles	Enables a user to open the security editor To work with security profiles, you also need rights granted on the universe.
Share projects	Enables a user to share a local project and to synchronize a shared project with the local project
Create, modify, or delete connections	• Enables a user to create and to delete secured connections from the Published Resources view • Enables a user to edit connections in the connection editor • Enables a user to publish connections to a repository
Publish universes	Enables a user to publish universes to a repository
Retrieve universes	Enables a user to retrieve published universes in a local project that will be edited
Save for all users	Enables a user to save for all users when retrieving universes
Compute statistics	Enables a user to select tables and columns on which to calculate and publish statistics
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

33.3.10.6 Alerting

Right	Description
Trigger Alerts	Enables a user to trigger alert events. To trigger an alert for a document, the following additional rights are required: • "View" and "Schedule" rights on the document • "View" and "Trigger" rights on the corresponding event

Right	Description
Subscribe to Objects	Enables a user to subscribe to an alert event. To subscribe to an event, the following additional rights are required: • "View" right on the corresponding event • "Subscribe" right on the user's own account To subscribe to an alert in a document, the following additional rights are required: • "View" right on the document • "View Instance" right on the document • "View" right on the corresponding event • "Subscribe" right on the user's own account
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

33.3.10.7 BI Admin Cockpit

Rights	Description
Allow access to BI Admin Cockpit	Enables you to access BI Admin Cockpit in CMC
Allow access to Monitoring	Enables you to access Monitoring in BI Admin Cockpit
Allow access to Visual Difference	Enables you to access Visual Difference in BI Admin Cockpit
Visual Difference - Create Comparison	Enables you to create new comparisons between info objects in Visual Difference
Visual Difference - Delete Comparison	Enables you to delete the previous comparisons in Visual Difference
Visual Difference - Rerun Comparison	Enables you to run the previously created comparisons again in Visual Difference
Visual Difference - View Comparison	Enables you to view a comparison in Visual Difference

34 Server Properties Appendix

34.1 About the server properties appendix

This server properties appendix lists and describes properties that can be set for each BI platform server.

34.1.1 Common Server Properties

The server properties described in this section apply to all server types.

Request Port Properties

Property	Description	Default Value
Server Name	The name of the server.	The default value is the name of the node that the server is on plus the name of the server.
ID, CUID	The short ID and cluster unique ID of the server. Read-only.	These values are auto-generated.
Node	The name of the node where the server is located.	This values is specified during installation.
Description	The server's description	The default value is the name of the server.
Command Line Parameters	The command-line parameters for the server.	The default value depends on the type of server.
Request Port	Specifies the port from which the server receives requests. In an environment with firewalls, configure the server to only listen to requests on ports that are open on the firewall. If you are specifying a port for the server, ensure that the port is not already taking by another process. **Note** If *Auto assign* is selected, the server binds to a dynamically allocated port. This means that a random port number is allocated to the server each time the server is restarted.	By default *Auto assign* is set to **TRUE**, and the *Request Port* is empty.
Auto assign	Specifies whether the server binds to a dynamically allocated port whenever the server is restarted. To bind the server to a specific port, set *Auto Assign* to **FALSE** and specify a valid *Request Port*.	The default value is **TRUE**.

Auto-Start Properties

Property	Description	Default Value
Automatically start this server when the Server Intelligence Agent starts	Specifies whether the server is automatically started when the Server Intelligence Agent (SIA) starts or restarts. If this value is set to **FALSE** and the SIA starts or restarts, the server remains stopped.	The default value is **TRUE**.

Host Identifier Properties

Property	Description	Default Value
Auto assign	Specifies whether the server binds to a network interface that is automatically assigned. If set to **FALSE**, the server binds to a specific network interface. If set to **TRUE**, the server accepts requests on the first available IP Address. On multihomed machines, you can specify a particular network interface to bind to by setting this value to **FALSE** and providing a valid hostname or IP Address.	The default value is **TRUE**.
Hostname	The hostname of the network interface that the server binds to. If a host name is specified, the server accepts requests on all IP Addresses associated with the host name.	By default *Auto assign* is set to **TRUE**, and the *Hostname* is empty.
IP Address	The IP Address of the network interface that the server binds to. Both IPv4 and IPv6 protocols are supported. If an IP Address is specified, the server accepts requests on the IP Address only.	By default *Auto assign* is set to **TRUE**, and the *IP Address* is empty.

Configuration Template Properties

Property	Description	Default Value
Use Configuration Template	Specifies whether to use a configuration template.	The default value is **FALSE**.
Restore System Defaults	Specifies whether to restore the original default settings for this server.	The default value is **FALSE**.
Set Configuration Template	Specifies whether to use the current service's settings as a configuration template for all services of the same type. If set to **TRUE**, all services of the same type that you have specified to *Use Configuration Template* are immediately reconfigured to use the settings of the current service.	The default value is **FALSE**.

TraceLog Service Properties

Property	Description	Default Value
Log Level	Specifies the minimum severity of messages that you want to be recorded, and determines how much information is recorded in the server log file. Possible log threshold levels are: • *Unspecified* • *None* • *Low* • *Medium* • *High*	The default value is **`Unspecified`**.

34.1.2 Core Services properties

The Core services category includes the following servers:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Event Server
- Input File Repository Server
- Output File Repository Server

Adaptive Job Server properties

General properties

Property	Description	Default Value
Temporary Directory	Specifies the directory where temporary files are created on when necessary. You may encounter performance issues if this directory does not have adequate disk space. For better performance, ensure that this directory is located on a local disk. **Note** You must restart the server for changes to take effect.	%DefaultDataDir%

The Adaptive Job Server can host a number of different services. Each service has the following properties

Service properties

Property	Description	Default Value
Maximum Concurrent Jobs	Specifies the number of concurrent independent processes (child processes) that the server allows. You can adjust the maximum number of jobs to suit your reporting environment. The default setting is acceptable for most reporting scenarios. The ideal setting for your reporting environment depends on your hardware configuration, database software, and reporting requirements.	5
Maximum Child Requests	Specifies the number of jobs the child will process before restarting.	100

Adaptive Processing Server properties

General properties

Property	Description	Default Value
Service Startup Timeout (seconds)	Specifies the amount of time, in seconds, that the server will wait for services to start. If a service fails to start within the time specified, there are two possible reasons: • The service failed, for example, because a required resource such as a database could not be found, or the service encountered a port conflict. • The service could not start within the specified time, for example, because the system is too slow. To find the reason, check the server log file. If the service could not start within the time specified, consider increasing this value.	1200

Client Auditing Proxy Service properties

Property	Description	Default Value
No configuration properties		

Security Token Service properties

Property	Description	Default Value
No configuration properties		

Insight to Action Service properties

Metric	Description	
Maximum Number of Active Connections Per User Session	The maximum number of connections with the SAP server available for a user for a given time. When a user opens a report or dashboard that is RRI capable, a connection with the SAP server will be established to determine the available RRI targets.	20
Maximum Number of Idle Connections Per User Session	The number of idle connections to keep open and re-use for subsequent RRI requests. Increasing this setting will allocate additional system resources.	20
Maximum Connection Wait Time (in seconds)	The amount of time the Insight to Action framework should wait for a response from the SAP Server before timing out (in seconds).	30

Publishing Service properties

Property	Description	Default value
Thread Pool Size	Specifies how many scope batch processing threads can run at the same time. If the value of this property is set to "0", the thread pool size is determined using a formula based on the number of CPU cores in the current machine.	0

Translation Service properties

Property	Description	Default value
No configuration properties		

Monitoring Service properties

Property	Description	Default value
No configuration properties		

Platform Search Service properties

Property	Description	Default value
No configuration properties		

Publishing Post Processing Service properties

Property	Description	Default value
No configuration properties		

Central Management Server properties

> **Note**
>
> When you modify any of these server properties, you must restart the server for the changes to take effect.

Central Management Service properties

Property	Description	Default Value
Name Server Port	Specifies the port on which the CMS listens to initial name service requests.	6400
System Database Connections Requested	Specifies the number of CMS system database connections that the CMS attempts to establish. If the server cannot establish all of the requested database connection, the CMS continues to function but at a reduced performance, since fewer concurrent requests can be served simultaneously. The CMS will attempt to establish additional connections, until the requested number of connection is established. The CMS's *Established System Database Connections* metric shows the current number of established connections.	14
Auto Reconnect to System Database	Specifies whether the CMS automatically attempts to reestablish a connection to the CMS database in the event of a service disruption. If this value is set to **FALSE**, you are able to check the integrity of the CMS database before resuming operations; you must restart the CMS to reestablish the database connection.	**TRUE**

Single Sign-on Service properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection to a datasource is valid before expiring. This applies to Windows AD users running reports that are configured for Windows AD SSO to the datasource.	86400

Event Server properties

Event Service properties

Property	Description	Default Value
Event Poll Interval (seconds)	Specifies how often the server polls for a file that triggers an event, in seconds.	10 The range of allowed values is 1 to 1200 seconds.
Cleanup Interval (minutes)	Specifies how often cleanup utility runs, in minutes.	20

Input File Repository Server properties

Input Filestore Service properties

Property	Description	Default Value
File Store Directory	Specifies the directory where file repository objects are stored. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultInputFRSDir/%
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space. To ensure better performance, it is recommended that the *Temporary Directory* is located on the same file system as the *File Store Directory*.	%DefaultInputFRS-Dir/temp%
Maximum Idle Time (minutes)	Specifies the length of time that the server waits before it closes inactive connections. Setting a value that is too low can cause a user's request to be closed prematurely. Setting a value that is too high can cause excessive consumption of system resources such as processing time and disk space.	10
Maximum Retries for File Access	Specifies the number of times the server tries to access a file.	1
Virus Scan Adapter File Location	Specifies the absolute path of the virus scan adapter file location.	

Output File Repository Server properties

Output Filestore Service properties

Property	Description	Default Value
File Store Directory	Specifies the directory where file repository objects are stored. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultOutputFRSDir/%

Property	Description	Default Value
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultOutputFRS-Dir/temp%
Maximum Idle Time (minutes)	Specifies the length of time that the server waits before it closes inactive connections. Setting a value that is too low can cause a user's request to be closed prematurely. Setting a value that is too high can cause excessive consumption of system resources such as processing time and disk space.	10
Maximum Retries for File Access	Specifies the number of times the server tries to access a file.	1

34.1.3 Connectivity Services Properties

The Connectivity service category includes the following services:

- Native Connectivity Service (hosted in standalone server)
- Native Connectivity Service (32-bit hosted in standalone server)
- Adaptive Connectivity Service (hosted in APS)

All services share the same configuration settings.

Excel Data Access Service Properties

Property	Description	Default Value
Excel Data Access Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	The default value is 1200 seconds.
Excel Data Access Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the *Excel Data Access Cleanup Timeout (in seconds)* property.	The default value is 600 seconds.

Service Operation Properties

Property	Description	Default Value
Remember You do not need to restart the server after changing the following Service Operation Properties.		

Property	Description	Default Value
Connection Pooling	Either enables or disables the connection pool. Possible values are: • Enabled - With Timeout • Enabled - Without Timeout • Disabled **Note** The connection pool is a caching functionality that maintains connections in a reusable state for improving server performance.	Enabled - With Timeout
Connection Pool Timeout	Specifies the maximum idle time for connections in the pool (in minutes). **Note** This property is equivalent to the `Max Pool Time` parameter of the `cs.cfg` file. Disabling the pool is equivalent to `Max Pool Time` set to `0`. Enabling the pool without timeout is equivalent to `Max Pool Time` set to `-1`. Refer to *Data Access Guide* for more information.	**`60`**
Transient Object Inactivity Timeout	Specifies how many minutes to keep an unused temporary object in the server. The object is removed afterwards and its resources are reclaimed.	**`60`**
Transient Object Timer Interval	Specifies the time between activity checks (in minutes). At regular intervals, the server searches for candidate objects for removal.	**`5`**
Enable HTTP Chunking	Either enables or disables the HTTP chunking. **Note** The HTTP chunking is relevant to 3-tier deployment only. It impacts the open/refresh document performance, because bigger responses mean less roundtrips when fetching large documents. Disabling the HTTP chunking is equivalent to *HTTP Chunk Size* set to **`0`**.	Enabled
HTTP Chunk Size	Specifies the size of the HTTP responses emitted by the server (in kilobytes).	**`64`**

Low Level Tracing Properties

Property	Description	Default Value
	→ Remember You do not need to restart the server after changing the following Low Level Tracing Properties.	
Enable Job Tracing	Enables the tracing of Connection Server jobs. **ⓘ Note** It requires *Log Level* property to be set to *High*.	Disabled
Enable Middleware Tracing	Enables the tracing of all middleware. To trace specific middleware, you must configure the `cs.cfg` file and restart the server. **ⓘ Note** It requires *Log Level* property to be set to *High*.	Disabled

Active Data Sources Properties

Property	Description	Default Value
	⚠ Caution You must restart the server after changing the following Active Data Sources Properties.	
Activate Data Source	Allows you to select the data sources for which you want connections. This property works as a filter for drivers. You specify the active data sources to load the drivers you want to use. **⚠ Caution** The default server behavior is to load all available drivers. Use this setting to specialize servers. It is particularly useful when you deploy multiple CORBA servers on your network. **→ Remember** Only drivers for selected data sources are loaded. All the others are ignored. If you do not select any data sources, the server loads all available drivers. **ⓘ Note** Verify in the server metrics that the selected data sources have been activated. The network layers and databases are displayed under *Connection Service Metrics*.	Unchecked

Property	Description	Default Value
Network Layer	Specifies the network layer used by the connection. **Note** Only the non-localized name is considered. You can find the list of available network layers in the `driver.cfg` file, which is located in the `<connectionserver-install-dir>\connectionServer` directory.	• **ODBC** for native CORBA servers • **JDBC** for Adaptive CORBA server
Database	Specifies the database used by the connection. **Note** Only the non-localized name is considered. Database names can be regular expressions if they are pure ASCII strings. Patterns use GNU regexp syntax. Use the `.*` pattern to match any character. For example, the `MS SQL Server.*$` expression means all MS SQL Server databases are used. For more information about regular expressions, refer to the PERL website at http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions .	The field is empty until you enter a database name.

Custom Data Access Service Properties

Property	Description	Default Value
Custom Data Access Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	The default value is 1200 seconds.
Custom Data Access Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the *Custom Data Access Cleanup Timeout (in seconds)* property.	The default value is 600 seconds.

Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Promotion Management Service Properties

Property	Description	Default Value
No configuration properties		

Promotion Management ClearCase Service Properties

Property	Description	Default Value
No configuration properties		

Visual Difference Service Properties

Property	Description	Default Value
No configuration properties		

Related Information

Common Server Properties [page 1059]

34.1.4 Crystal Reports Services Properties

The Crystal Reports service category includes the following servers:

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Crystal Reports 2025 Report Application Server Properties
- Crystal Reports 2025 Processing Server

Crystal Reports Cache Server Properties

Any properties that apply to both Crystal Reports Cache Servers and Crystal Reports Processing Servers should be set to the same value. For example, if you set the *Viewer Refresh Always Yields Current Data* setting to **TRUE** on the Cache Server, you should set the same property to **TRUE** on the Processing Server.

> **Note**
>
> When you modify any of these server properties, you must restart the server for the changes to take effect.

Crystal Reports Cache Service Properties

Property	Description	Default Value
Viewer Refresh Always Yields Current Data	Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings. To specify a value on the report object, select the report in the CMC, and click *Default Settings* > *Viewing Server Group*.	The default value is **FALSE**.

Property	Description	Default Value
Share Report Data Between Clients	Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is **TRUE**.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Crystal Reports Cache Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 20 minutes.
Security Cache Timeout (minutes)	Specifies the amount of time, in minutes, that the server uses cached logon credentials, report parameters, and database connection information to serve requests before querying the CMS.	The default value is 20 minutes.
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand reports. If the server receives a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (perhaps because important data changes very frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is 0 seconds.
Maximum Cache Size (KB)	Specifies the amount of hard disk space (in KB) that is used to cache reports. A large cache size may be necessary if the server needs to handle large numbers of reports, or reports that are especially complex.	The default value is 256000 KB.
Cache Files Directory	Specifies the location of the cache file directory.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Java VM Arguments	Specifies the command-line arguments that can be supplied to the JVM.	The default value is empty.
DLL Name	Specifies the name of the document-type plug-in that is currently loaded. This property is read-only.	rasprocReport

Crystal Reports Processing Server Properties

Any properties that apply to both Crystal Reports Cache Servers and Crystal Reports Processing Servers should be set to the same value. For example, if you set the *Viewer Refresh Always Yields Current Data* setting to **TRUE** on the Cache Server, you should set the same property to **TRUE** on the Processing Server.

> **Note**
>
> When you modify any of these server properties, you must restart the server for the changes to take effect.

Crystal Reports Processing Service Properties

Property	Description	Default Value
Idle Job Timeout (minutes)	Specifies the length of time, in minutes, that the Crystal Reports Processing Server waits between requests for a given job.	The default value is 20 minutes.
Maximum Lifetime Jobs Per Child	Specifies the maximum number of jobs that each child process can manage per lifetime.	The default value is 1000.
Viewer Refresh Always Yields Current Data	Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings. To specify a value on the report object, select the report in the CMC, and click *Default Settings* > *Viewing Server Group*.	The default value is **FALSE**.
Share Report Data Between Clients	Specifies whether report data is shared between different clients. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is **TRUE**.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Crystal Reports Processing Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 20 minutes.
Maximum Concurrent Jobs (0 for automatic)	Specifies the maximum number of independent jobs allowed to run concurrently on the Crystal Reports Processing Server. If the value of this property is set to "0", the server applies a suitable value, based on the CPU and memory of the machine that the server is running on.	The default value is 0.

Property	Description	Default Value
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand reports. If the server receives a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (perhaps because important data changes very frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is 0.
Maximum Number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessary wasted by idle child processes.	The default value is 1 child.
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java Class Path	The name and path of the Java classes that are required by the server.	%CommonJavaLibDir%/procCR.jar
Java Child VM Arguments	Specifies the command-line arguments that are supplied to child processes that are created by the server.	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Crystal Reports 2025 Report Application Server Properties

> **Note**
>
> When you modify any of these properties, you must restart the server for the changes to take effect.

Crystal Reports 2025 Viewing and Modification Service Properties

Property	Description	Default Value
Allow Report Jobs to Stay Connected to the Database until the Report Job is Closed	Specifies whether the report job will remain connected to the database until the process has been executed.	The default value is **FALSE**.
Browse Data Size (records)	Specifies the number of distinct records returned from the database when browsing through a particular field's values. The data is retrieved first from the client's cache - if it is available - and then from the server's cache. If the data is not in either cache, it is retrieved from the database.	The default value is 100 records.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Report Application Server (RAS) waits for requests from an idle client before timing out. Setting a value too low can cause a user's request to be closed prematurely, and setting a value that is too high can affect the server's scalability (for instance, if the `ReportClientDocument` object is not closed explicitly, the server will be waiting unnecessarily for an idle job to close).	The default value is 30 minutes.
Batch Size (records)	Specifies how many rows from the result set are returned by the database during each data transfer. For example, if 500 records are requested, and the Batch Size property is set to 100 records, the data will be returned in 5 separate batches of 100 rows. To improve the performance of your RAS, you must understand your network environment, database, and the type of requests in order to set the appropriate batch size.	The default value is 100 records.
Number of database records to read when previewing or refreshing a report (-1 for unlimited)	Specifies the number of database records that will be read when viewing or refreshing a report. This setting limits the number of records that the server retrieves from the database when a user runs a query or report. This setting is useful when you want to prevent users from running on-demand reports that return excessively large record sets. You may prefer to schedule such reports, both to make the reports available more quickly to users and to reduce the load on your database from these large queries.	The default value is 20000 records.

Property	Description	Default Value
Maximum Concurrent Report Jobs (0 for unlimited)	Specifies the maximum number of independent jobs allowed to run concurrently on the RAS.	The default value is 75 jobs.
Oldest on-demand data given to a client (minutes)	Specifies the amount of time, in minutes, an on-demand report will serve cached report data.	The default value is 20 minutes.
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Crystal Reports 2025 Processing Server Properties

Note

When you modify any of these properties, you must restart the server for the changes to take effect.

Crystal Reports 2025 Processing Service Properties

Property	Description	Default Value
Idle Job Timeout (minutes)	Specifies the length of time, in minutes, that the Crystal Reports Processing Server waits between requests for a given job.	The default value is 20 minutes.
Maximum Lifetime Jobs Per Child	Specifies the maximum number of jobs that each child process can manage per lifetime.	The default value is 1000.
Viewer Refresh Always Yields Current Data	Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings. To specify a value on the report object, select the report in the CMC, and click *Default Settings* > *Viewing Server Group*.	The default value is **FALSE**.

Property	Description	Default Value
Share Report Data Between Clients	Specifies whether report data is shared between different clients. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is **TRUE**.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Crystal Reports Processing Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 20 minutes.
Maximum Concurrent Jobs (0 for automatic)	Specifies the maximum number of independent jobs allowed to run concurrently on the Crystal Reports Processing Server. If the value of this property is set to "0", the server applies a suitable value, based on the CPU and memory of the machine that the server is running on.	The default value is 0.
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand reports. If the server receives a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (perhaps because important data changes very frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is 0.
Maximum Number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessary wasted by idle child processes.	The default value is 1 child.

Property	Description	Default Value
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultDataDir%/CrystalReports2025ProcessingServer/temp
Allow Report Jobs to Stay Connected to the Database until the Report Job is Closed	Specifies whether the report job will remain connected to the database until the job is closed.	The default value is FALSE.
Database Records Read When Previewing or Refreshing (0 for unlimited)	Specifies the number of database records that will be read when viewing or refreshing a report. This setting limits the number of records that the server retrieves from the database when a user runs a query or report. This setting is useful when you want to prevent users from running on-demand reports that return excessively large record sets. You may prefer to schedule such reports, both to make the reports available more quickly to users and to reduce the load on your database from these large queries.	The default value is 20000.

Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

34.1.5 Data Federation Services Properties

The Data Federation services category includes the Adaptive Processing Server:

Data Federation Service Properties

Property	Description	Default Value
Max Connections	Specifies the maximum number of connections allowed on the server.	The default value is 32767.
Execution Pool Size	Specifies the maximum number of queries that can be executed in parallel at a given moment.	The default value is 10.
Connection Inactivity Timeout	Specifies the amount of time in seconds after which an inactive connection is closed.	The default value is 10800 seconds.
Statement Inactivity Timeout	Specifies the amount of time in seconds after which an inactive query statement is closed.	The default value is 600 seconds.

34.1.6 Web Intelligence Services properties

The Web Intelligence services category includes the following servers:

- Adaptive Processing Server
- Web Intelligence Processing Server

Adaptive Processing Server settings

Command Line Parameters

Property	Description	Default Value
Expand to Level	Specifies the level to which data is retrieved from BEx queries. By default, hierarchies are not expanded to a given level. Level00 is always the default level. You can change this behavior by adding this parameter to the command line, but if the value is set too high, Web Intelligence retrieves all of the hierarchy data, which can affect the performance and stability of the system.	`-Dsap.sl.bics.expandToLevel=n` n can be any integer between 0 and 99. If n=0, or if this parameter is not specified, hierarchies will not use the Expand to Level parameter.
Selection Option variable selection	Specifies the selection option for variable selection. If this property is set to interval, then the text box is not available and users can only enter start and end values in the Prompts dialog box. If this property is set to multivalue, then the "Type a value" text box is available and users can enter values for BW Selection Option variables. **Note** This property does not update local installations of Web Intelligence Rich Client. See the "Web Intelligence Rich Client Installation Guide" for information on updating the local registry for such installations.	`-Dsap.sl.bics.variableComplexSelectionMapping=n` where n can be either interval or multivalue. **Note** Prior to BI 4.1 SP05, the default value for this option was interval. If you add this property to the Adaptive Processing Server settings and set it to multivalue, then the following actions need to be done on existing documents: • A document needs to be purged. • The default values for query prompts need to be changed so that it is compatible with multivalue selection.

Web Intelligence Monitoring Service properties

Property	Description	Default Value
Enable Monitoring	Specifies whether monitoring is enabled for the service.	**TRUE**

Property	Description	Default Value
Monitoring Thread Loop Delay (seconds)	Specifies the amount of time, in seconds, between attempts that the service makes to ping clients.	300
Default Monitored Resource Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	1200
Default Monitored Resource Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the Default Monitored Resource Cleanup Timeout property.	600
Enable Service Profiling		**TRUE**
Enable Service Activity Monitoring		**TRUE**

Visualization Service properties

Property	Description	Default Value
Visualization Engine Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	1200
Visualization Engine Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the *Visualization Engine Cleanup Timeout (in seconds)* property.	600

Rebean Service properties

Property	Description	Default value
No configuration properties		

Document Recovery Service properties

Property	Description	Default value
No configuration properties		

DSL Bridge Service properties

Property	Description	Default value
DSLBridge Engine Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	1200

Web Intelligence Processing Server properties

The Web Intelligence Processing Server properties are grouped into the following services:

- Information Engine

- Web Intelligence Core
- Web Intelligence Processing
- Web Intelligence Common

Threshold settings are described in separate tables.

Information Engine Service properties

Property	Description	Default Value
Enable List of Values Cache	Specifies whether caching is enabled for List of Values on the Web Intelligence Processing Server.	**TRUE**
List of Values Batch Size (entries)	Specifies the maximum number of entries (or values) for each List of Values batch.	1000
Maximum Custom Sort Size (entries)	Specifies the maximum number of entries in the custom sort.	100
Universe Cache Maximum Size (Universes)	Specifies the number of universes to be cached on the Web Intelligence Processing Server.	20
Maximum List of Values Size (entries)	Specifies the maximum number of entries (or values) for each List of Values.	50000

Web Intelligence Core Service properties

Property	Description	Default Value
Timeout Before Recycling (seconds)	Specifies the time, in seconds, the server is idle before the Server Intelligence Agent (SIA) stops and restarts the server when the total number of documents processed is above the value specified with the *Maximum Documents Before Recycling* property.	1200
Idle Document Timeout (seconds)	Specifies the amount of time, in seconds, before the Web Intelligence Processing Server session will be swapped. Therefore, when the client is not generating requests during this period of time, the session will be swapped onto the hard disk, freeing up resources for an active session.	300 The valid range is 100 to 10000 seconds.
Server Polling Interval (seconds)	Specifies the interval, in seconds, that must pass before the server polls for new thread requests. When the server is in the polling phase, it performs cleanup actions like swapping unused documents to keep the server memory under the upper memory threshold.	120
Maximum Documents per User	Specifies the maximum number of active sessions (Web Intelligence documents) that can be associated with a user at any given time. Therefore, if 5, then the user can use up to 5 active sessions at once.	5 The valid range is 1 to 20.
Maximum Documents Before Recycling	Specifies the number of Web Intelligence documents that can be processed before the server will be considered for recycling. If the number of processed documents has been reached, and the server is idle, then the server is closed and the Server Intelligence Agent (SIA) starts a new instance of the server. However, there will be a time delay before a new instance of the server is started. The time delay is defined by the *Timeout Before Recycling* property.	50

Property	Description	Default Value
Allow Document Map Maximum Size Errors	Specifies whether the `<Maximum Connections>` property is restricted. If this property is enabled, then the value set for the `<Maximum Connections>` property is recognized by the server; otherwise the property is disregarded.	**TRUE**
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the server waits for a request from an idle connection. Setting a value that is too low can cause a request to close prematurely. Setting a value that is too high can caused requests to be queued while the server waits for idle requests to be closed.	20
Maximum Connections	Specifies the maximum number of simultaneous sessions that can be opened at one time. This is an approximate number; this setting does not count the inactive sessions that are swapped, or the session that is created to analyze the number of sessions. If this limit is reached and no other server is available to handle the request, the user will receive an error message. **Note** The `<Allow Document Map Maximum Size Errors>` property must be enabled for this property to be recognized by the server.	200 The valid range is 5 to 65535.
Enable Memory Analysis	Specifies whether memory analysis is enabled. If this property is enabled then the following properties will be active and recognized by the server: • `<Memory Maximum Threshold>` • `<Memory Upper Threshold>` • `<Memory Lower Threshold>` When the server's process memory is above the `<Memory Upper Threshold>`, the only operation that is allowed is saving documents. When the process memory is above the `<Memory Maximum Threshold>`, all operations stop and fail.	**TRUE**
Memory Lower Threshold (MB)	Specifies the lower threshold for memory consumption.	**3500**
Memory Upper Threshold (MB)	Specifies the upper threshold for memory consumption.	**4500**
Memory Maximum Threshold (MB)	Specifies the maximum threshold for memory consumption.	**6000**
Enable APS Service Monitoring	Enables monitoring of the server by the APS service, hosted on the Adaptive processing server.	**TRUE**
Retry Count on APS Service ping failure	Specifies the number of times the server will try to reach the APS Service before deciding that it is unable to reach it.	3
APS Service Monitoring Thread Period	Specifies the period of delay between attempts to reach the APS Service.	300

Property	Description	Default Value
Enable Current Activity Logs	Specifies whether complete traces are generated in the server's log files. **Note** This property should be enabled only for debugging purposes when troubleshooting issues. Set to **FALSE** during normal operations.	**FALSE**

Web Intelligence Processing Service properties

Property	Description	Default Value
Enable use of HTTP URL	Specifies whether the server is able to access files that are stored remotely.	**TRUE**
Proxy value	Specifies the address of your network's proxy server. It is only necessary to specify a value if your network has a proxy server and you attempting to access files that are stored remotely.	Blank

Web Intelligence Common Service properties

Property	Description	Default Value
Cache Timeout (minutes)	Specifies the amount of time, in minutes, before the contents of the document cache will be cleared. The timeout depends on the most recent access date per document.	4370
Document Cache Clean-up Interval (minutes)	Specifies the time interval, in minutes, that the document cache is scanned and is checked against the `<Maximum Document Cache Size>`, `<Maximum Document Cache Reduction Space>`, and `<Maximum Document in Cache>` settings.	120
Disable Cache Sharing	Specifies whether cache sharing is disabled. By default cache sharing is enabled; which means that all Web Intelligence Processing Server instances will share the same cache. However, if you prefer to have one cache per instance of Web Intelligence Processing Server then you should enable this property.	**FALSE**
Enable Document Cache	Specifies whether the document cache is enabled. If the property is enabled, then the cache can be pre-loaded with scheduled Web Intelligence documents.	**TRUE**
Enable Real-Time Cache	Specifies whether the real-time cache is enabled. If the property is enabled, then the cache can be loaded dynamically. Therefore, the Web Intelligence Processing Server caches Web Intelligence documents when they are viewed. The server also caches the documents when they run as a scheduled job, if the pre-cache was enabled in the document.	**TRUE**
Maximum Document Cache Size (KB)	Specifies the maximum size of the document cache. Once this limit is reached the document cache will be cleared based on the `<Maximum Document Cache Reduction Space>` property.	1000000
Maximum Document Cache Reduction Space (percent)	Specifies the percentage of cache that is emptied to allow newer actions and results to be stored in the cache. Documents with the oldest "last access time" are purged.	70

Property	Description	Default Value
Maximum Character Stream Size (MB)	Specifies the maximum character stream size sent to the Web Intelligence client. **Note** If the *Maximum Character Stream Size* property is exceeded, then the Web Intelligence document will not be created and the client will receive an error message.	5 The valid range is 1 to 4095 MB.
Binary Stream Maximum Size (MB)	Specifies the maximum size, in MB, of a binary stream sent to the Web Intelligence client. **Note** If the *Binary Stream Maximum Size* property is exceeded, then the Web Intelligence document will not be created and the client will receive an error message.	50 The valid range is 1 to 4095 MB.
Images Directory	Specifies the location of the images directory.	Blank
Output Cache Directory	Specifies the location of the cache.	Blank

General properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	86400

Related Information

Web Intelligence Server Memory Threshold Settings [page 1083]

34.1.6.1 Web Intelligence Server Memory Threshold Settings

The following sections describe what happens on a Web Intelligence server when the Memory Maximum Threshold, Memory Upper Threshold, or Memory Lower Thresholds are reached.

Memory Lower Threshold

If the `<Memory Lower Threshold>` limit is reached, the server swaps out inactive documents onto the hard disk allocating additional memory for the documents which are active. Each user is allowed to have up to one active document instead of `<Maximum Documents per User>`.

Memory Upper Threshold

If this `<Memory Upper Threshold>` is reached, the following server actions will take place in order to free resources and protect the server:

- The server will reject new connections and new client calls. Only the option to *Save* Web Intelligence documents will be allowed. Users that request an action will receive a `Server Busy` message, and they will be notified that they should save any pending changes.
- The server will turn on system cleanup to free enough resources so that the amount of allocated memory is below the limit set by the `<Memory Upper Threshold>` property.
- The server tries to close read-only documents.
- If not enough memory was freed during system cleanup then the server will begin to close documents that are in *Editing* mode. The server will begin to close documents based on the LIFO protocol; the most recent active document will be purged from memory first. The server will continue to close documents until a safe level is reached; this level is based on the following calculation: `<Memory Upper Threshold>` - (20%*(`<Memory Upper Threshold>`)). For example, if the Memory Upper Threshold property is set to 4500MB then the safe level would be:

  ```
  4500MB - .20*4500MB = 3600MB
  ```

  The server cannot close documents when a client call is running. Any document that is refreshed or exported to another format or any other time consuming operation will not be closed when the server reaches this threshold. If the server cannot recover enough memory and is still above the `<Memory Upper Threshold>`, it restarts.

Memory Maximum Threshold

If the <Memory Maximum Threshold> limit is reached, all current operations abort. All client calls will be terminated. Once the a call terminates, the corresponding document will be closed.

35 Server Metrics Appendix

35.1 About the Server Metrics Appendix

In this appendix unless otherwise stated, the term server refers to an SAP BusinessObjects server, and not to the machine that the BI platform is installed or running on.

Server metrics are not available on servers that are not running.

In addition to the metrics described in this appendix, the Monitoring application can also monitor these server states:

Server State	Description
Health State	The Health State indicates the general health of a server. These are the possible values: • 0 = Red (Danger) • 1 = Amber (Caution) • 2 = Green (Healthy)
Server Enabled State	This state indicates whether a server is enabled or disabled. These are the possible values: • 0 = Disabled • 1 = Enabled
Server Running State	This state indicates the running state of a server. These are the possible values: • 0 = STOPPED • 1 = STARTING • 2 = INITIALIZING • 3 = RUNNING • 4 = STOPPING • 5 = FAILED • 6 = RUNNING_WITH_ERRORS • 7 = RUNNING_WITH_WARNINGS

35.1.1 Common Server Metrics

The following metrics describe the machine that the specified server is running on.

Machine-specific metrics

Metric	Description
Machine Name	The host name of the machine that the server is running on.
Operating System	The operating system of the machine that the server is running on.
CPU Type	The type of Central Processing Units of the machine that the server is running on. This metric is not available on Adaptive Processing Servers .
CPUs	The number of CPUs that are available to the server. On multi-core hardware, this metric may report the number of logical CPUs, and not the number of physical processors. This metric is not available on Adaptive Processing Servers.
Number of Cores	Displays the number of cores in a machine, where the BI platform server is hosted.
RAM (MB)	The amount of memory in megabytes that is available on the machine that the server is running on. This metric is not available on Adaptive Processing Servers.
Local Time	The local time.
Disk Size (GB)	The size of the disk that the BI platform is installed on, in gigabytes. This metric is not available on Adaptive Processing Servers.
Used Disk Space (GB)	The amount of used space on the disk, in gigabytes, that the BI platform is installed on. This includes disk space that is used by other programs on the machine, and not just space used by the BI platform. This metric is not available on Adaptive Processing Servers .

The following metrics describe the specified SAP BusinessObjects server.

Server-specific metrics

Metric	Description
Name Server	The name and port number of the CMS server that this server publishes its address to.
Registered Name	The internal name of the server. This is not the name that appears on the *Servers* screen of the CMC.
Version	The version of the server.
Start Time	The time that the server was most recently started.
PID	The unique Process ID number for the server. The operating system of the machine that the server is running on generates the PID. The PID can be used to identify the specific server.
Host Name	A comma-separated list of host names that are currently being used by the server.
Host IP Address	A comma-separated list of IP Addresses that the server listens for requests on.
Request Port	The port from which the server receives requests from other servers. If the server is listening to requests on more than one IP Address, the request port for the server will always be the same. If any other process uses this request port, the server will not start. Ensure that other processes do not use this port.

Metric	Description
Busy Server Threads	The number of server threads that are currently servicing a request. If this number is the same as the maximum thread pool size of the server, it indicates that the system can't process additional requests in parallel and that new requests may have to wait for busy threads to become available.

Auditing Metrics

Metric	Description
Current Number of Auditing Events in the Queue	The number of auditing events that an Auditee has recorded, but which have not yet been retrieved by the CMS Auditor. If this number increases without bound, it could indicate that Auditing is not configured correctly or that the system is heavily loaded and generating audit events faster than the Auditor can retrieve them. **Note** When stopping a server, first disable it and wait for this metric to reach "0". Otherwise you may have auditing events that remain in the queue and do not reach the Auditing Data Store until the server is restarted and the CMS polls for them.

Logging Service Metrics

Metric	Description
Logging Directory	Log files for the server are available in this location.

35.1.2 Central Management Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Central Management Servers (CMS).

Central Management Server Metrics

Metric	Description
Connection to Auditing Database is Established	Indicates whether the CMS has a healthy connection to the auditing database. A value of "1" indicates that there is a connection. A value of "0" indicates that there is no connection to the auditing database. If the CMS is an auditor, this value should be "1". If it is "0", investigate why a connection to the auditing database cannot be established.
CMS Auditor	Indicates if the CMS Is acting as an auditor. A value of "1" indicates that the CMS is acting as an auditor. A value of "0" indicates that the CMS is not acting as an auditor.
Auditing Database Connection Name	The name of the auditing database connection. This is not necessarily the name of the auditing database itself. If this metric is empty, it indicates that a connection to the auditing database cannot be established.
Auditing Database User Name	The name of the user account used to connect to the auditing database.

Metric	Description
Auditing Database Last Updated On	The most recent date and time that the CMS successfully started to retrieve events from an auditee. If the CMS is an auditor, this metric must show a time that is close to the time that the "Metrics" screen is loaded. If this value is more than two hours prior to the time that the screen is loaded, it may indicate that auditing is not working properly.
Auditing Thread Last Polling Cycle Duration (seconds)	The duration of the last polling cycle in seconds. This indicates the maximum delay for event data to reach the auditing database during the previous polling cycle. • A value of less than 20 minutes indicates a healthy system. • A value between 20 minutes and 2 hours indicates a busy system. • A value of greater than 2 hours indicates a very busy system. If this state persists and you consider the delay too long, it is recommended that you either update your deployment to all the auditing database to receive data at a higher rate or decrease the number of auditing events that your system tracks.
Auditing Thread Utilization	The percentage of the polling cycle the auditor CMS spends collecting data from auditees. The remainder is time spent resting between polls. If this value this reaches 100%, the auditor is still collecting data from the auditees when the next poll is due to begin. This may cause delays in the events reaching the auditing database. If the Thread Utilization frequently reaches 100%, and remains at this rate for several days, it is recommend you either update your deployment to allow the auditing database to receive data at a higher rate, or decrease the number of auditing events that your system tracks.
Clustered CMS Servers	A semicolon-separated list of the host names and port numbers of the running Central Management Servers in the cluster.
Number of Sessions Established by Concurrent Users	The total number of sessions for users with concurrent licensing.
Number of Sessions Established by Named Users	The total number of sessions for users with named licensing.
Peak Number of User Sessions Since Startup	The peak number of concurrent user sessions that the CMS has handled since it was started.
Number of Sessions Established by Servers	The number of concurrent sessions that BI platform servers have created with the CMS. If this number is greater than 250, create an additional CMS.
Number of Sessions Established by All Users	The number of concurrent user sessions that are being handled by the CMS when the *Metrics* screen loads. The larger this number is, the larger the number of users that are using the system is. If this number is greater than 250, create an additional CMS.
Failed Jobs	The number of failed jobs in the system.
Pending Jobs	The number of jobs that are scheduled, but not ready, to run because the scheduled time or event has not arrived.
Running Jobs	The number of currently running jobs.
Completed Jobs	The number of completed jobs in the system.

Metric	Description
Waiting Jobs	The number of jobs in the system that are scheduled and waiting for free resources.
Concurrent User Licenses	The number of Concurrent User licenses as indicated by the key code.
Named User Licenses	The number of Named User licenses as indicated by the key code
Build Date	The build date of the CMS.
System Database Connection Name	The name of the CMS system database connection. This is not necessarily the name of the CMS system database itself.
System Database Server Name	The name of the server where the CMS system database is running. This is not necessarily the name of the CMS system database itself.
System Database User Name	The name of the user account used to connect to the CMS system database.
Data Source Name	The name of the CMS system database connection.
Build Number	The build number of the CMS. This number can be used to identify the version of SAP BusinessObjects Business Intelligence platform that you have installed.
Product Version	The product version of the CMS.
Resource Version	The resource version of the CMS.
Average Commit Response Time Since Startup (msec)	The average length of time in milliseconds that it took the CMS to perform commit operations since the server was started. A response time greater than 1000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Average Query Response Time Since Startup (msec)	The average length of time in milliseconds that it took the CMS to perform query operations since the server was started. A response time greater than 1000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Longest Commit Response Time Since Startup (msec)	The longest length of time in milliseconds that the it took the CMS to perform commit operations since the server was started. A response time greater than 10000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Longest Query Response Time Since Startup (msec)	The longest length of time in milliseconds that the it took the CMS to perform query operations since the server was started. A response time greater than 10000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Number of Commits Since Startup	The number of commits to the CMS system database since the server was started.
Number of Queries Since Startup	The total number of database queries since the server was started. A large number may indicate a more active or heavily loaded system.
Number of User Logons Since Startup	The number of user logons since the server was started. A large number may indicate a more active or heavily loaded system.

Metric	Description
Established System Database Connections	The number of connections to the CMS system database that the CMS was able to establish. If a database connection is lost, the CMS attempts to restore the connection. If the number of established database connections is consistently lower than the number of system database connections specified by the *System Database Connections Requested* property (*Central Management Service* area of the *Properties* screen), it may indicate that the CMS can't acquire additional connections, and that the system is not functioning optimally. A potential solution is to configure the database server to allow more database connections for the CMS.
Currently Used System Database Connections	The number of connections to the CMS system database that the CMS is currently using. The number of connections that are being currently used may be smaller than or equal to the number of established system database connections. If the number of established connections and the number of used connections are identical for some time, this may indicate a bottleneck. Increasing the value for the *System Database Connections Requested* property on the *Properties* screen may improve the performance of the CMS. Tuning the CMS system database may also improve performance.
Pending System Database Requests	The number of requests for the CMS system database that are waiting for an available connection. If this number is high, consider increasing the value for the *System Database Connections Requested* property. Tuning the CMS system database may also improve performance.
Number of Objects in CMS System Cache	The total number of objects that are currently in the CMS system cache.
Number of Objects in CMS System DB	The total number of objects that are currently in the CMS system database.
Existing Concurrent User Accounts	The total number of existing users with concurrent licensing in the cluster.
Existing Named User Accounts	The total number of existing users with named licensing in the cluster.

35.1.3 Connection Server Metrics

The following metrics are specific to the Connection Server.

Connectivity Service metrics

Metric	Description
Data Sources	Lists in a table the data sources activated via the *Properties* page. Displays the following information for each network layer and database pair: • *Status* (*Loaded* or *Failed!*): current status of the driver • *Available Connections: number of pool connections that can be used* • *Jobs (CORBA): number of jobs that are being processed (2-tier deployment)* • *Jobs (HTTP): number of jobs that are being processed processing (web tier deployment)* **Note** For more information about connection pools, refer to the *Data Access Guide*.

35.1.4 Event Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Event Servers.

Event Service Metrics

Metric	Description
List of Monitored Files	A table that lists the files that are being monitored by the Event Server. The "Filename" column displays the name and path of the file. The "Last Notified Time" column displays the latest timestamp of when the server did a poll and found that the file exists.
Monitored Files	The total number of files that are being monitored by the Event Server.

35.1.5 File Repository Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Input and Output File Repository Servers.

Filestore Service Metrics

Metric	Description
Active Files	The number of files in the File Repository Server that are currently being accessed.
Data Written (MB)	The total number of megabytes written to files on the server.
Data Sent (MB)	The total number of megabytes read from files on the server.
List of Active Files	A table that displays the files in the File Repository Server that are currently being accessed.

Metric	Description
Active Connections	The total number of active connections from clients and to other servers.
Available Disk Space in Root Directory (GB)	The total amount of available space on the disk containing the server's executable file, in gigabytes.
Free Disk Space in Root Directory (GB)	The total amount of free space on the disk containing the server's executable file, in gigabytes.
Total Disk Space in Root Directory (GB)	The total disk space on the disk containing the server's executable file, in gigabytes.
Available Disk Space in Root Directory (%)	The amount of available disk space, in percentage, on the disk containing the server's executable file.

35.1.6 Adaptive Processing Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Adaptive Processing Servers.

Adaptive Processing Server metrics

Metric	Description
Threads in Transport Layer	The total number of threads in all thread pools of the transport layer.
Transport Layer Thread Pool Size	The total number of shared transport layer threads. These threads can be used by any of the hosted services on the Adaptive Processing Server.
Available Processors	The number of processors that are available to the Java Virtual Machine (JVM) on which the server is running.
Maximum Memory (MB)	The maximum amount of memory, in megabytes, that the Java virtual machine will attempt to use.
Free Memory (MB)	The amount of memory, in megabytes, that is available to the JVM for allocating new objects.
Total Memory (MB)	The total amount of memory, in megabytes, in the Java virtual machine. This value may vary over time, depending on the host environment.
CPU Usage Percentage (last 5 minutes)	The percentage of total CPU time used by the server during the previous five minutes. For example, if a single thread fully utilizes one CPU of a four-CPU system, the utilization is 25%. All processors allocated to the JVM are considered. A value of greater than 80% may indicate a CPU bottleneck.
CPU Usage Percentage (last 15 minutes)	The percentage of total CPU time used by the server during the previous 15 minutes. For example, if a single thread fully utilizes one CPU of a four-CPU system, the utilization is 25%. All processors allocated to the JVM are considered. A value of greater than 70% may indicate a bottleneck.

Metric	Description
Percentage of stopped system during GC (last 5 minutes)	Percentages of stopped system while Garbage Collections (GC) were running during the last five minutes. In this state all APS services are prevented from executing while the virtual machine performs a critical stage of garbage collection that requires exclusive access. Generally, a low single-digit value should be the normal behavior, even under load. A double-digit value over time might indicate an issue of low throughput and needs to be investigated.
Percentage of stopped system during GC (last 15 minutes)	Percentages of stopped system while Garbage Collections (GC) were running during the last 15 minutes. In this state all APS services are prevented from executing while the virtual machine performs a critical stage of garbage collection that requires exclusive access. Generally, a low single-digit value should be the normal behavior, even under load. A double-digit value over time might indicate an issue of low throughput and needs to be investigated.
Number of page faults during GC (last 5 minutes)	The number of page faults that have occurred while Garbage Collections were running during the previous five minutes. Any value greater than 0 indicates a system under heavy load and low memory conditions.
Number of page faults during GC (last 15 minutes)	The number of page faults that have occurred while Garbage Collections were running during the last 15 minutes. Any value greater than 0 indicates a system under heavy load and low memory conditions.
Number of Full GCs	The number of full Garbage Collections since the server has started. A rapid increase in this value may indicate a system under low memory conditions.
JVM Lock Contention Count	The number of synchronized objects that have threads that are waiting for access. Any value consistently greater than 0 may indicate threads that will not run again. Initiate a Thread Dump to obtain more information about the cause of the problem.
JVM Debug Info	Debugging information about the SAP Java Virtual Machine, including the state, port, and attached client, if available.
JVM Version Info	Version information about the SAP Java Virtual Machine.
JVM Deadlocked Threads Counter	The number of threads that are deadlocked. Any value greater than 0 indicates threads that will not run again. Initiate a Thread Dump to obtain more information about the cause of the problem.
JVM Trace Flags	The trace flags that are currently turned on for the JVM. This indicates the level of tracing of the JVM.
Services	A comma-separated list of the services that the server hosts.

DSL Bridge Service metrics

Metric	Description
DSLServiceMetrics.queryCount	The number of data requests that are open between clients and the service
DSLServiceMetrics.activeConnectionCount	The number of connections that are currently open between clients and the service.
DSLServiceMetrics.activeSessionCount	The number of sessions that are currently open between clients and the service.

Metric	Description
DSLServiceMetrics.activeOLAPConnection Count	The number of connections that are currently open between OLAP clients and the service.

Client Auditing Proxy Service metrics

Metric	Description
Number of Audit Events Received Since Server Startup	The number of client auditing events that the service has received since it was started. This metric can be used to verify that client auditing has been configured correctly. Values greater than "0" indicate that auditing events from clients are being successfully routed through this Client Auditing Service.

Platform Search Service metrics

Metric	Description
Number of Successful Extraction Attempts since the Service Start	The number of successful attempts for extracting documents since the Platform Search Service was started.
Last Index Update Timestamp	The date and time when the last index update happened.
Last Content Store Generation Timestamp	The date and time when the last content store was generated.
Number of failed extraction attempts since the service start	The number of failed attempts for extracting documents since the Platform Search Service was started.
Service Available	TRUE if the service is available. Otherwise FALSE.
Indexing Running	TRUE if the indexing is running. Otherwise FALSE.
Number of Documents Indexed	The displays the number of documents that were indexed since the service was started.

Data Federation Service metrics

Metric	Description
Number of Running Queries	The total number of running queries (consuming memory or not).
Number of Connections	The total number of user connections to data federation query engine.
Total Bytes Transferred from Data Sources	The amount of data read from the data sources (in bytes).
Total Records Transferred from Data Sources	The total number of rows read from the data sources.
Total Bytes Produced by Query Execution	The amount of data produced as output of queries (in bytes).
Total Records Produced by Query Execution	The total number of rows produced as output of queries.
Number of Queries Consuming Memory	The total number of running queries consuming memory.
Total Bytes of Memory Used by Query Execution	The amount of memory currently used by the running queries (in bytes).
Total Bytes of Disk Used by Query Execution	The amount of disk currently used by the running queries (in bytes).
Number of Queries Using Disk	The total number of running queries using disk.
Number of Queries Waiting for Resources	The total number of running queries currently waiting for execution.
Number of Active Threads	The total number of active threads used for used for execution of requests.

Metric	Description
Total Bytes of Memory Used by Metadata Cache	The amount of memory used for caching metadata, statistics and connectors configuration (in bytes).
Number of Failed Queries	The total number of failed queries (exception raised).
Number of Queries in Query Analyze Step	The total number of running queries currently in analyze step.
Number of Queries in Query Optimization Step	The total number of running queries currently in optimization step.
Number of Queries in Query Execution Step	The total number of running queries currently in execution step.
Number of Loaded Connectors	The total number of connectors loaded in the service.
Number of Active Connections to Loaded Connectors	The total number of active connections to connectors loaded in the service.
Data Federation Service is available	*TRUE* if the service is available. Otherwise, *FALSE*.

Connectivity Service metrics

Metric	Description
Data Sources	Lists in a table the data sources activated on the *Properties* page. Displays the following information for each network layer and database pair: • Status ("Loaded" or "Failed"): The current status of the driver • Available connections: The number of pool connections that can be used • Jobs (CORBA): The number of jobs that are being processed (in a 2-tier deployment) • Jobs (HTTP: The number of jobs that are being processed (in a web-tier deployment) For more information about connection pools, see the *Data Access Guide*.

Monitoring Service metrics

Metric	Description
Average Watch State Computation Time for Last 15 Cycles (msec)	The average time required for computing the watch state over the last 15 cycles, for this monitoring service instance.
Number of User Created Metrics	The total number of user-created metrics in the cluster, for all users.
Number of Watches	The total number of watches in the cluster, including both disabled and enabled watches.
serviceBean.monitoringAppPropEnabled	TRUE if the Monitoring application is enabled. Otherwise FALSE. This metric matches the setting on the Monitoring Application Properties page in the CMC.
Monitoring Metrics Refresh Interval (seconds)	The refresh interval currently being used by this monitoring service instance. At service start-up, this metric is initialized to the setting on the Monitoring Application Properties page in the CMC at that time, so at other times the metric may be different from the current setting on the CMC page.
Service Available	TRUE if this monitoring service is active. Otherwise FALSE. Only one monitoring service is active in the cluster.

Metric	Description
Number of Trended Metrics	The total number of metrics currently being recorded into the monitoring database.

35.1.7 Adaptive Job Server Metrics

Job Server Metrics

Metric	Description
Received Job Requests	The number of jobs that were supposed to have run on the server.
Concurrent Jobs	The number of jobs that are currently running on the server. If this number is high, the server is busy.
Peak Jobs	The maximum number of concurrent jobs that have run at the same time on the server. This number never goes down until the server is restarted.
Failed Job Creations	The number of jobs that failed on the server.
Temporary Directory	The directory where temporary files are created. This can be specified on the *Properties* screen for the server. You may encounter issues if this directory does not have adequate disk space.
File System Destination Default Settings Valid	*TRUE* if the server is able to send documents to the File System Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
FTP Destination Default Settings Valid	*TRUE* if the server is able to send documents to the FTP Server Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
SFTP Destination Default Settings Valid	*TRUE* if the server is able to send documents to the SFTP Server Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*. You may encounter issues if the fingerprint does not match correctly with SFTP server.
Inbox Destination Default Settings Valid	*TRUE* if the server is able to send objects to the Inbox Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
Email Destination Default Settings Valid	*TRUE* if the server is able to send objects to the Email Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
Scheduling Services	A table that displays the services that are running on the server.
Children	A table that displays the child processes that are running on the server.

The following table describes the metrics for each Scheduling Service that is running on the server.

Scheduling Service Metrics

Metric	Description
Scheduling Service	The name of the service.
Received Job Requests	The number of jobs that were supposed to have run on the service.

Metric	Description
Concurrent Jobs	The number of concurrent jobs that are currently running on the service. If this number is high, the service is busy.
Peak Jobs	The maximum number of concurrent jobs that have run at the same time on the service.
Maximum Concurrent Jobs Allowed	The number of concurrent independent processes (child processes) that the service allows. This can be specified on the *Properties* screen for the server.
Failed Job Creations	The number of jobs that failed on the service.

The following table describes the metrics for each child process that is running on the server.

Child Metrics

Metric	Description
Scheduling Service	The name of the child process.
PID	The child process's identifier.
Received Job Requests	The number of jobs that were supposed to have run on the child process.
Concurrent Jobs	The number of concurrent jobs that are currently running on the child process. Normally this number must be “1”.
Peak Jobs	The maximum number of concurrent jobs that have run at the same time on the child process.
Maximum Jobs Allowed	The number of concurrent jobs that the child process allows.
Comm. Failures	The number of communication failures with the parent Adaptive Job Server that have occurred. If this number is large, the child process will restart.
Initializing	*TRUE* if the child process is in the process of initializing. Otherwise, *FALSE*.
Shutting Down	*TRUE* if the child process is in the process of shutting down. Otherwise, *FALSE*.

35.1.8 Crystal Reports Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports Processing and Crystal Reports 2025 Processing Servers.

Crystal Reports Processing Server Metrics

Metric	Description
Open Jobs	A table listing of the jobs that are currently being run on the server. The table includes the ID and Name of the document, the name of the user running the job, the date that the document was last accessed, and the amount of time that the job has been running.
Number of Requests Served	The total number of requests that the server has served since it started.

Metric	Description
Number of Open Jobs	The number of currently jobs that the server and its child processes are currently processing.
Object Type	The type of InfoObject that the server primarily deals with. The value for this metric does not change.
Average Processing Time (ms)	The average time, in milliseconds, the server has spent processing the last 500 requests that the server has received. If this number is consistently high and growing, consider creating additional servers on other machines.
Maximum Processing Time (ms)	The maximum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Minimum Processing Time (ms)	The minimum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Number of Queued Requests	The number of requests that are either waiting to be processed or are being processed. If this number is consistently high and growing, consider creating additional servers on other machines.
Object Dll Name	The name of the processing plug-in for the server. The value of this metric does not change.
Number of Open Connections	The number of connections that are currently open between the server and clients.
Request Failure Rate	The number of requests that the server failed to process as a percentage of the last 500 requests that the server has received.
Data Transferred (KB)	The total amount of data, in kilobytes, that have been transferred to clients since the server was started.
Number of Requests Failed	The number of requests that the server was unable to complete since the server started.
Maximum Number of Child Processes	The maximum number of concurrent child processes that are allowed on the server.

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports Cache Servers.

Crystal Reports Cache Server Metrics

Metric	Description
Cache Hit Rate (%)	The percentage of requests, over the last 500 requests, that have been served with cached data.
Connected Processing Servers	A table listing of the Crystal Reports Processing servers in your deployment. The table lists the name of the server and the number of connections that are currently open with the server.
Number of Requests Served	The total number of requests that the server has served since it started.
Object Type	The type of InfoObject that the server primarily deals with. The value for this metric does not change.

Metric	Description
Average Processing Time (msec)	The average time, in milliseconds, the server has spent processing the last 500 requests that the server has received. If this number is consistently high and growing, consider creating additional servers on other machines.
Maximum Processing Time (msec)	The maximum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Minimum Processing Time (msec)	The minimum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Number of Queued Requests	The number of requests that are either waiting to be processed or are being processed. If this number is consistently high and growing, consider creating additional servers on other machines.
Object Dll Name	The name of the processing plug-in for the server. The value of this metric does not change.
Cache Size	The amount of data, in kilobytes, that is currently being cached by the server on the disk.
Number of Open Connections	The number of connections that are currently open between the server and clients.
Data Transferred (KB)	The total amount of data, in kilobytes, that have been transferred to clients since the server was started.

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports 2025 Report Application Servers.

Crystal Reports 2025 Report Application Server Metrics

Metric	Description
metric_currentdoccount **Note** This metric appears as "document_s_" on the Monitoring page in the CMC.	The number of documents that are currently being processed by the server.
metric_totaldoccount **Note** This metric appears as "document_s_" on the Monitoring page in the CMC.	The number of documents that have been processed by the server since it started.

Metric	Description
metric_currentagentthreadcount **Note** This metric appears as "agent thread_s_" on the Monitoring page in the CMC.	The number of threads that are currently being processed by the server.
metric_totalagentthreadcount **Note** This metric appears as "agent thread_s_" on the Monitoring page in the CMC.	The number of threads that have been processed by the server since it started.

35.1.9 Web Intelligence Server Metrics

Web Intelligence Processing Service Metrics

Metric	Description
Cache size (Kb)	The current amount, in kilobytes, of data that is stored in the cache.
Number of out-of-date documents in cache	The number of documents deleted from the cache because there were too old, since the server was started.
Cache high mark count	The number of times that the cache has reached the maximum size allowed on the server since it was started.
CPU usage (%)	The percentage of total CPU time spent by the server since the server was started.
Total CPU time (seconds)	The total CPU time, in seconds, spent by the server since it was started.
Memory high threshold count	The number of times that the high memory threshold has been reached on the server since it was started.
Memory max threshold count	The number of times that the maximum memory threshold has been reached on the server since it was started.
Virtual memory size (Mb)	The total amount of memory, in megabytes, that are assigned to the server.
Current number of client calls	The current number of CORBA calls that the server is processing.
Number of remote extension errors	The number of times the server has failed to connect to a remote extension service hosted by an Adaptive Processing Server.
Current number of tasks	The current number of tasks that are being executed on the server.
Total number of client calls	The total number of CORBA calls that the server has received since it was started.
Total number of tasks	The total number of tasks that have been executed on the server since it was started.

Metric	Description
Idle time (seconds)	The amount of time, in seconds, that have elapsed since the last request that the server has received from a client.
Current number of active sessions	The current number of sessions that are able to accept requests from clients.
Number of documents opened from cache	The number of documents for which the last request result has been directly read from the cache.
Number of documents	The number of documents that are currently open on the server.
Current number of sessions	The current number of sessions that have been created on the server.
Number of document swap	The number of documents for which a cleanup thread has scheduled swap requests.
Number of swapped documents	The number of documents that have been swapped by swap requests.
Number of sessions timeout	The number of sessions that have timed out since the server was started.
Total number of sessions	The number of sessions that have been created on the server since the server was started.
Number of users	The total number of users that are connected to the server.
Number of active threads	The number of threads serving requests received by the server (asynchronism threadpool).
Total number of threads	The total number of threads that have been created since the server was started (asynchronism threadpool).

36 Server and Node Placeholder Appendix

36.1 Server and node placeholders

With the exception of *%SERVER_FRIENDLY_NAME%* and *%SERVER_NAME%*, these placeholders apply to all of the servers on the same node.

> **Note**
>
> The following placeholders can be edited at the node level. Descriptions and default values can be found in the above table. Placeholders that do not appear in this list are read-only.
>
> - *%DefaultAuditingDir%*
> - *%DefaultDataDir%*
> - *%DefaultLoggingDir%*
> - *%IntroscopeAgentEnableInstrumentation%*
> - *%IntroscopeAgentEnterpriseManagerHost%*
> - *%IntroscopeAgentEnterpriseManagerPort%*
> - *%IntroscopeAgentEnterpriseManagerTransport%*
> - *%NCSInstrumentLevelThreshold%*
> - *%SMDAgentHost%*
> - *%SMDAgentPort%*

> **Caution**
>
> Placeholders other than intended for editing should not be changed in any means. System Administrator should ensure that only the right person from the Administrator group (who are intended for the Node management) should have the edit rights on the Node. All other users including other members of the administrator group should be restricted to view/manage the Node objects by applying the proper security rights. In case if any of the placeholder values is corrupted accidentally and CMS is not coming up, refer to the following SAP Note 3269127.

> **Note**
>
> Please refer to the following SAP Knowledge Base Article 3278916 to know how to restrict placeholders being modified to avoid possible malicious interference with the BI landscape.

Placeholders

Placeholder	Description	Default values
%AuditingDatabaseConnection%	The Auditing Database connection used by the CMS.	This value is specified during installation.

Placeholder	Description	Default values
%AuditingDatabaseDriver%	The type of database driver that is used to connect to the auditing database.	On Windows, the default value is sqlserverauditdbss.
%BINDIR%	The folder where SAP BusinessObjects Business Intelligence platform 64-bit binaries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/`
%BINDIR32%	The folder where SAP BusinessObjects Business Intelligence platform 32-bit binaries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/`
%CACHESERVER_EXE%	The name of the executable for the Crystal Reports Cache Server.	On Windows, `crcache.exe`. On UNIX, `boe_crcached.bin`.
%CMS_EXE%	The name of the executable for the Central Management Server.	On Windows, `cms.exe`. On UNIX, `boe_cmsd`.
%CONNECTIONSERVER32_EXE%	The name of the executable for the 32-bit Connection Server.	On Windows, `ConnectionServer32.exe`. On UNIX, `ConnectionServer32`.
%CONNECTIONSERVER_DIR%	The root folder of the Connection Server.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer`
%CONNECTIONSERVER_EXE%	The name of the executable for the 64-bit Connection Server.	On Windows, `ConnectionServer.exe`. On UNIX, `ConnectionServer`.
%CRCPP_BINDIR%	The directory where Crystal Reports C++ server binaries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. On UNIX, the directory will be similar to: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.

Placeholder	Description	Default values
%CRCPP_DefaultWorkingDir%	The default working directory for Crystal Reports C++ servers.	On Windows, `<INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. On UNIX, the directory will be similar to: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRYSTALRAS_EXE%	The Name of the executable for the Report Application Server.	On Windows, `crystalras.exe`. On UNIX, `boe_crystalrasd`.
%CR_ODBCINI%	The name and path of the `.odbc.ini` file is located.	On UNIX, `<INSTALLDIR>/bobje/odbc.ini`. On Windows, this is an empty string.
%CommonJavaBundlesDir%	The folder where shared OSGI bundles are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bundles`.
%CommonJavaLibDir%	The folder where the common Java libraries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib`.
%DLLEXT%	The default extension of a `.dll` or `.so` file.	On Windows, `.dll`. On UNIX, `.so`.
%DLLPATH%	The name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories where the interpreter will search for executable files.	On Windows, "Path". On UNIX, "LD_LIBRARY_PATH".
%DLLPATH32%	On Solaris 32-bit systems, The name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories where the interpreter will search for executable files.	On Solaris machines, "LD_LIBRARY_PATH_32". This placeholder is an empty string on other operating systems.
%DLLPATH64%	On Solaris 64-bit systems, the name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories there the interpreter will search for executable files.	On Solaris machines, "LD_LIBRARY_PATH_64". This placeholder is an empty string on other operating systems.

Placeholder	Description	Default values
%DLLPREFIX%	The default prefix of a `.dll` or `.so` file.	On UNIX, “lib”. This placeholder is an empty string on Windows machines.
%DLLPRELOAD%	The name of the LD_PRELOAD environment variable for the platform.	On UNIX *LD_PRELOAD*. This placeholder is an empty string on Windows machines.
%DP%	The path delimiter.	On Windows, “;”. On UNIX, “:”.
%DefaultAuditingDir%	The directory where Auditing temporary files are written. For optimum performance, this location should be on the server's local drive.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Auditing`. On UNIX, `<INSTALLDIR>/sap_bobj/data/Auditing/`.
%DefaultDataDir%	The temporary directory used by the Job Server.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data`. On UNIX, `<INSTALLDIR>/sap_bobj/data/`.
%DefaultInputFRSDir%	The root folder of the Input File Repository Server.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input`. On UNIX, `<INSTALLDIR>/sap_bobj/data/frsinput`.
%DefaultLoggingDir%	The location where the log files are stored.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`. On UNIX, `<INSTALLDIR>/sap_bobj/logging`.
%DefaultOutputFRSDir%	The root folder of the Output File Repository Server.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output`. On UNIX, `<INSTALLDIR>/sap_bobj/data/frsoutput`.
%DefaultWorkingDir%	The working directory for 64-bit servers	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>`.
%DefaultWorkingDir32%	The working directory for 32-bit servers.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>`.
%EPM_LD_PRELOAD_ONCE%	The name of the LD_PRELOAD_ONCE environment variable for the platform.	$LD_PRELOAD_ONCE$

Placeholder	Description	Default values
%EVENTSERVER_EXE%	The name of the executable for the Event Server.	On Windows, `EventServer.exe`. On UNIX, `boe_eventsd`.
%EXEEXT%	The default extension of executable files.	On Windows, `.exe`. This placeholder is unavailable on UNIX.
%EXEPATH%	The name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories there the interpreter will search for executable files.	On Windows, "Path". On UNIX, "PATH".
%EnterpriseDir%	The location where 64-bit SAP BusinessObjects Business Intelligence platform is installed.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40`.
%EnterpriseDir32%	The location where 32-bitSAP BusinessObjects Business Intelligence platform is installed.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40`.
%ExternalJavaLibDir%	The folder where external, third-party Java libraries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/external`.
%FILESERVER_EXE%	The name of the executable for the File Server	On Windows, `fileserver.exe`. On UNIX, `boe_filesd`.
%HOARD_PATH%	The location of the memory manager.	By default, this is empty.
%HOARD_PRELOAD%	Specifies whether to preload the memory manager.	By default, this is empty.
%INSTALLROOTDIR%	The folder where 64-bit SAP BusinessObjects Business Intelligence platform is installed.	This value is specified during installation.
%INSTALLROOTDIR32%	The folder where 32-bit SAP BusinessObjects Business Intelligence platform is installed.	This value is specified during installation.
%IntroscopeAgentEnableInstrumentation%	Indicates whether instrumentation for Java servers using Introscope Agent Enterprise Manager is enabled.	Possible values are TRUE or FALSE, depending on whether Introscope Agent Enterprise Manager was enabled when SAP BusinessObjects Business Intelligence platform was installed.
%IntroscopeAgentEnterpriseManagerHost%	The Introscope Agent Enterprise Manager hostname to which instrumentation data is sent.	This value is specified during installation.

Placeholder	Description	Default values
%IntroscopeAgentEnterpriseManagerPort%	The Introscope Agent Enterprise Manager port to which instrumentation data is sent.	This value is specified during installation.
%IntroscopeAgentEnterpriseManagerTransport%	The transport that is used when sending instrumentation data to the Introscope Agent Enterprise Manager. Allowed values are: • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through HTTP.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through HTTPS.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through SSL.	com.wily.isengard.postoffice-hub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through TCP.	com.wily.isengard.postoffice-hub.link.net.DefaultSocketFactory
%IntroscopeDir%	The folder where Introscope Agent Enterprise Manager is installed.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\wily`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily`.
%JAVAW_EXE%	The name of the executable for the Java Virtual Machine that has no console window.	On Windows, `javaw.exe`. On UNIX, `java`.
%JAVA_EXE%	The name of the executable for the Java Virtual Machine.	On Windows, `java.exe`. On UNIX, `java`.
%JOBSERVERCHILD_EXE%	The name of the executable for the Adaptive Job Server Child.	On Windows, `JobServerChild.exe`. On UNIX, `boe_jobcd`.
%JOBSERVER_EXE%	The name of the executable for the Adaptive Job Server.	On Windows, `JobServer.exe`. On UNIX, `boe_jobsd`.

Placeholder	Description	Default values
%JdkBinDir%	The folder where the JDK binaries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. On UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/bin`.
%JreBinDir%	The folder where the JRE binaries are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. On UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/bin`.
%JVM_ARCH_ENVIRONMENT%	Indicates whether the machine is running on the 32-bit or 64-bit JVM.	For 32-bit UNIX machines, the default value is "-d32". For 64-bit machines, the default value is "-d64". On Windows machines, this is an empty string.
%JVM_HEADLESS_MODE%	The command-line argument that specifies whether the JVM works in headless mode.	On Windows, -Djava.awt.headless=false. On UNIX, -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	The command-line parameters that specify what the JVM does when it encounters Out of Memory errors.	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	The command-line parameters that enable JVM extensions and set the JVM's instance number.	By default, this placeholder is empty.
%LANGUAGEPACKSDIR%	The folder where the deployment's language packs are installed.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`.
%LANGUAGEPACKSDIR32%	The folder where the deployment's language packs are installed on 32-bit systems.	. On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`.
%LSTDir%	The folder where LST configuration files are stored.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\lst`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst`.
%MDAS_JVM_OS_STACK_SIZE%	Specifies the JVM stack-size for the Multidimensional Analysis Service.	By default, this placeholder is empty.
%NCSInstrumentLevelThreshold%	The threshold level of trace logging for the NCS library.	By default, this value is 0.

Placeholder	Description	Default values
%PAGESERVER_EXE%	The name of the executable for the Crystal Reports 2025 Processing Server.	On Windows, `crproc.exe`. On UNIX, `boe_crprocd.bin`.
%PJSContainerDir%	The folder where APS Container JARS are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/container`.
%PJSServicesDir%	The folder where APS Service JARS are located.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/services`.
%Platform%	The operating system of the machine that SAP BI platform is running on.	The operating system of the machine that SAP BI platform is running on.
%Platform32%	The operating system of the machine that 32-bit SAP BI platform is running on.	The operating system of the machine that SAP BI platform is running on.
%RasBinDir%	The root folder of the Report Application Server.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras`.
%SERVER_FRIENDLY_NAME%	The full name of the server.	The full name of the server.
%SERVER_NAME%	The full name of the server.	The full name of the server.
%SMDAgentHost%	The SMD Agent hostname to which instrumentation data is sent.	This value is specified during installation.
%SMDAgentPort%	The SMD Agent port to which instrumentation data is sent.	This value is specified during installation.
%TRACE_CONFIGFILE_INI%	The name and path of the `BO_Trace.ini` file.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/BO-trace.ini`.
%WarFilesDir%	The location of web application files.	On Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps`. On UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/warfiles/webapps`.

Placeholder	Description	Default values
%WEBI_LD_PRELOAD%	The name of the LD_PRELOAD environment variable for the platform.	$LD_PRELOAD$
%WEBISERVER_EXE%	The name of the executable for the Web Intelligence Processing Server.	On Windows, `wireportserver.exe`. On UNIX, `WIReportServer`.
%WEBI_LD_PRELOAD_ONCE%	The name of the LD_PRELOAD_ONCE environment variable for the platform.	$LD_PRELOAD_ONCE$

Related Information

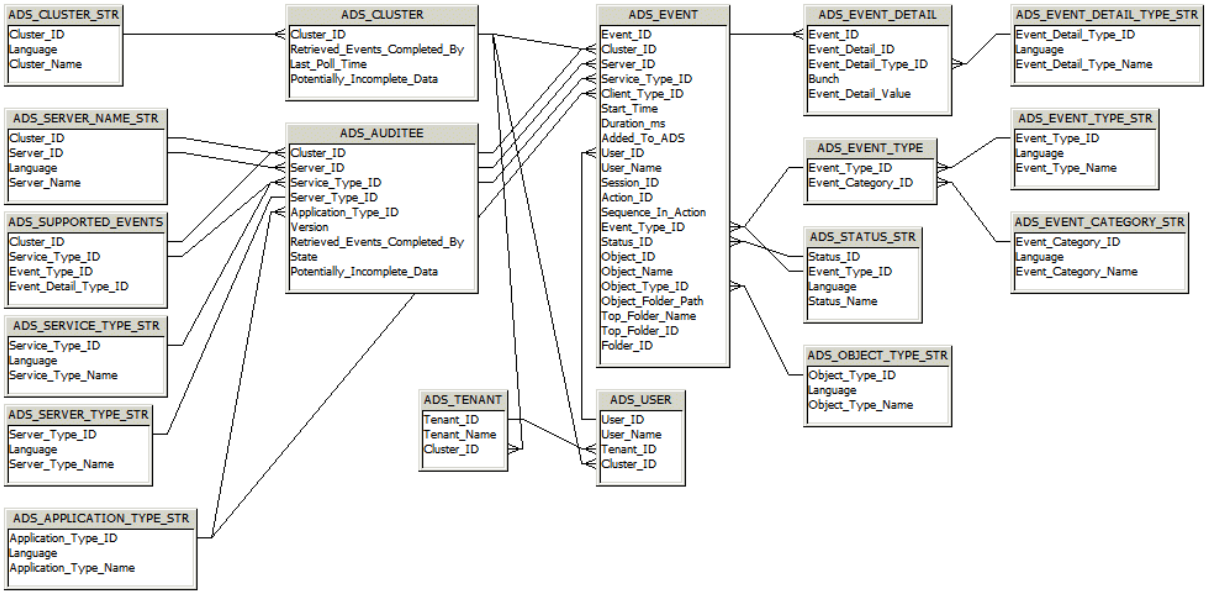
To view and edit the placeholders for a node [page 487]

37 Auditing Data Store Schema Appendix

37.1 Overview

This appendix is a reference for any report designers that will be accessing and reporting off the Auditing Data Store tables. The following diagram and table explanations show you the tables where the auditing data will be recorded and how those tables are related.

37.2 Schema diagram



37.3 Auditing Data Store Tables

ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

Column Name	Type	Description
Application_Type_ID	Character (64)	The application-type CUID for the application.
Language	Character (10)	Code for the language in which the application type is recorded; for example <EN>, or <DE>.
Application_Type_Name	Character (255)	The text name of the application type; Crystal Reports or Web Intelligence for example.

ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	The server-type CUID for the server that triggered the event.
Application_Type_ID	Character (64)	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS.
State	Integer	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	Shows if this auditee may have events that were not transferred to the ADS.

ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.

Column Name	Type	Description
Retrieved_Events_Completed_By	Datetime	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS.

ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	A unique ID of the cluster.
Language	Character (10)	Code for the language setting for the cluster, for example, `<EN>`, or `<DE>`.
Cluster_Name	Character (255)	The name of the cluster.

ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

Column Name	Type	Description
Event_ID	Character (64)	A unique ID generated for the event.
Cluster_ID	Character (64)	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	• The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID. • Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID.
Client_Type_ID	Character (64)	Records the Client Type ID of the client that established the session.

Column Name	Type	Description
Start_Time	Datetime	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	Duration of operation in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Added_to_ADS	Datetime	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	The CUID of the user who performed the action.
User_Name	Character (255)	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.
Event_Type_ID	Integer	Type of event (View or Save, for example).
Status_ID	Integer	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	CUID of the object that the operation was performed on.
Object_Name	Character (255)	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded.
Top_Folder_ID	Character (64)	The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded.

ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

Column Name	Type	Description
Event_Category_ID	Integer	The event-category ID.
Language	Character (10)	Code for the language that the event category name is recorded in; for example <EN>, or <DE>.
Event_Category_Name	Character (255)	The name of the event category.

ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

ADS_EVENT_DETAIL table

This table records event detail properties.

Column Name	Type	Description
Event_Detail_ID	Integer	GUID for the event detail.
Event_ID	Character (64)	Parent event GUID.
Event_Detail_Type_ID	Integer	Type of event detail.
Bunch	Integer	If the detail is part of a series, this is used to tie them together. For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of: • Prompt Name: Country • Prompt Value: USA Bunch 2 would consist of: • Prompt Name: State • Prompt Value: California • Prompt Value: Nevada
Event_Detail_Value	Character (long-text)	The value of the event detail.

ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

Column Name	Type	Description
Event_Detail_ID	Integer	The event detail-type ID for the event detail.
Language	Character (10)	Code for the language that the event detail name is recorded in; for example <EN>, or <DE>.
Event_Detail_Type_Name	Character (255)	The text name of the event detail type.

ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

Column Name	Type	Description
Event_Type_ID	Integer	The unique identifier for the type of event.
Event_Category_ID	Integer	Category of event. For example, common, Web Intelligence, or Life-Cycle Management.

ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

Column Name	Type	Description
Event_Type_ID	Integer	The event-type ID for the event.
Language	Character (10)	Code for the language that the event category name is recorded in; for example <EN>, or <DE>.
Event_Type_Name	Character (255)	The text name of the event type; View or Logon for example.

ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

Column Name	Type	Description
Object_Type_ID	Character (64)	Object-type CUID of the object
Language	Character (10)	Code for the language that the object type name is recorded in; for example <EN>, or <DE>.
Object_Type_Name	Character (255)	Name of the object type.

ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	The CUID of the server.
Language	Character (10)	Code for the language of the server name; for example <EN>, or <DE>.
Server_Name	Character (255)	The name of the server.

ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

Column Name	Type	Description
Service_Type_ID	Character (64)	The service-type or service-category CUID for the service.
Language	Character (10)	Code for the language the service-type name is recorded in, for example <EN>, or <DE>.
Service_Type_Name	Character (255)	The name of the service-type.

ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

Column Name	Type	Description
Status_ID	Integer	The numerical representation of the operation's status.
Event_Type_ID	Integer	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Code for the language that the event status is recorded in; for example <EN>, or <DE>.
Status_Name	Character (255)	A text description of the event's status; Succeeded or Failed, for example.

ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Column Name	Type	Description
Cluster_ID	Character (64)	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	CUID that identifies the type of event detail captured for that event (File Path, for example).

ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
Tenant_ID	Character (64)	The CUID of the tenant.
Tenant_Name	Character (255)	The name of the tenant.

ADS_USER Table

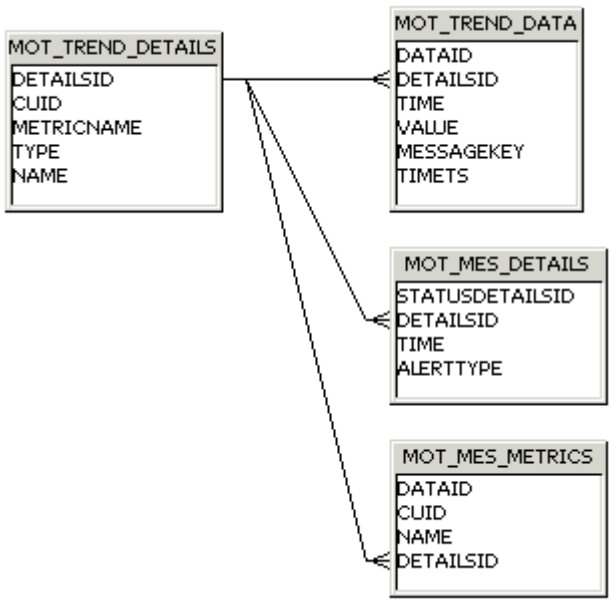
This table records the relationship between users and tenants.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
User_ID	Character (64)	The CUID of the user.
User_Name	Character (255)	The name of the user.
Tenant_ID	Character (64)	The CUID of the tenant.

38 Monitoring Database Schema Appendix

38.1 Trending database schema

The following Trending database diagram and table explanations show you the tables where the metric, probe, and watch data will be recorded and how these tables are related.



MOT_TREND_DETAILS

This table records information about managed entities, probes, and watches. For example, CUID and metric names.

Column Name	Type	Key	Description
DetailsId	INTEGER	Primary Key Autogenerated	
CUID	VARCHAR(64)	NA	CUID of the InfoObject that exposes the metric or is related to the metric
MetricName	VARCHAR(255)	NA	Name of the Metric
Type	VARCHAR(32)	NA	One of "Subscription", "ManagedEntityStatus", or "Probe"

Column Name	Type	Key	Description
Name	VARCHAR(255)	NA	Name of the watch when the type is "ManagedEntityStatus". Otherwise, default to the same string as in Type, except in all capital letters; for example, "PROBE" or "SUBSCRIPTION".

MOT_TREND_DATA

This table records the trending data from metrics, watches, and probes. For example, metric value and time.

Column Name	Type	Key	Description
DataId	INTEGER	Primary Key Autogenerated	
DetailsId	INTEGER	Foreign key (from MOT_TREND_DETAILS)	
Time or TimeT	BIGINT or NUMBER or FIXED Unix Epoch date	NA	Time at which data was collected
Value	FLOAT or DOUBLE or NUMBER	NA	Value of the metric / subscription
MessageKey	VARCHAR(32)	NA	Error message key or null if successful. For watch, it can also be either "watchEnabled" or "watchDisabled". It is a "key" because it is ultimately used to fetch localized messages before displaying the UI.
Ts	DATETIME or TIMESTAMP	NA	Time at which data is written to the database

MOT_MES_DETAILS

This table records the information about subscription breaches and alert delivery information. For example, breach time and alert delivery time.

Column Name	Type	Key	Description
StatusDetailsId	INTEGER	Primary Key Autogenerated	
DetailsId	INTEGER	Foreign key (from MOT_TREND_DETAILS)	

Column Name	Type	Key	Description
Time	BIGINT or NUMBER Unix Epoch date	NA	Time at which data was collected
AlertType	SMALLINT or NUMBER	NA	Subscription notification delivery type (for example, email)

MOT_MES_METRICS

This table records information about watches and the metrics belonging to the watch equations. Every metric belonging to the watch will have one entry in this table.

Column Name	Type	Key	Description
DataId	INTEGER	Primary Key Autogenerated	
DetailsId	INTEGER	Foreign key (from MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	NA	CUID of the watch
Name	VARCHAR(255)	NA	Name of the watch

39 System Copy Worksheet Appendix

39.1 System copy worksheet

Property	Value
Cluster key.	
Names of the nodes.	
The machine name and the BI platform installation folder for each machine in the deployment.	
The BI platform administrator password.	
CMS database connections, the user names and passwords associated with those connections for each machine in the deployment.	
Auditing database connections, the user names and passwords associated with those connections for each machine in the deployment.	
For each machine in the deployment, details of any other database client connections for each machine in the source system used by universes and reports.	
For each machine in the deployment, database client types and versions.	
The version, support package, and patch level.	
The file store locations for every Input FRS and Output FRS in the deployment.	
If you plan to copy Promotion Management, the location of the Promotion Management database folder and Subversion folders.	
If you plan on copying the monitoring database, the monitoring database folder.	
The semantic layer folder path.	

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.