PUBLIC

SAP BusinessObjects Business Intelligence platform

Document Version: 4.3 – 2020-06-12

Business Intelligence Platform CMC Help

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 The Central Management Console. 15
1.1 About the Central Management Console. 15
1.2 Logging on to the CMC. 16
1.3 Navigating the CMC. 16
1.4 Setting CMC preferences. 17

2 System Configuration Wizard. 18
2.1 Introduction to the System Configuration Wizard. 18
2.2 Specifying the products you use. 18
2.3 Choosing a deployment template. 20
2.4 Specifying data folder locations. 22
2.5 Reviewing your changes. 23
2.6 Log files and response files. 23
Using a response file. 24

3 Managing Users and Groups. 28
3.1 Managing Enterprise and general accounts. 28
To create a user account. 28
To modify a user account. 29
To delete a user account. 29
To create a new group. 30
To modify a group's properties. 30
To view group members. 31
To add subgroups. 31
To specify group membership. 32
To add users or user groups in bulk. 32
To delete a group. 33
To enable the Guest account. 33
To add the Customization tab to a user group. 34
Adding users to groups. 34
Changing password settings. 36
Enabling Trusted Authentication. 37
Granting access to users and groups. 38
Controlling access to user inboxes. 39
Setting BI launch pad preferences for user groups in the CMC 39
Setting Fiorified BI Launch pad preferences for user groups in the CMC. 41
3.2 Managing aliases. 43

To create a user and add a third-party alias. . . . 43
To create a new alias for an existing user. . . . 44
To assign an alias from another user. . . . 44
To delete an alias. . . . 45
To disable an alias. . . . 45

4 Setting Rights. . . . 47
4.1 Managing security settings for objects in the CMC. . . . 47
To view rights for a principal on an object. . . . 47
To assign principals to an access control list for an object. . . . 48
To modify security for a principal on an object. . . . 48
To set rights on a top-level folder in the BI platform. . . . 49
Checking security settings for a principal. . . . 49
4.2 Working with access levels. . . . 51
Choosing between *View* and *View On Demand* access levels. . . . 53
To copy an existing access level. . . . 54
To create a new access level. . . . 54
To rename an access level. . . . 55
To delete an access level. . . . 55
To modify rights in an access level. . . . 55
Tracing the relationship between access levels and objects. . . . 56
Managing access levels across sites. . . . 57
4.3 Breaking inheritance. . . . 58
To disable inheritance. . . . 59

5 Authentication. . . . 60
5.1 Overview. . . . 60
Authentication options in the BI platform. . . . 60
5.2 Enterprise authentication. . . . 60
Enterprise authentication. . . . 60
Enterprise authentication settings. . . . 61
5.3 LDAP authentication. . . . 63
LDAP authentication. . . . 63
Configuring SSL settings for LDAP Server or Mutual Authentication 66
Configuring the LDAP plug-in for SiteMinder 70
Mapping LDAP groups. . . . 71
5.4 Windows AD authentication. . . . 73
Windows AD authentication. . . . 73
Windows AD Security plug-in. . . . 74
To configure Windows AD authentication 75
To map Windows AD groups. . . . 78
5.5 SAP authentication. . . . 79

SAP Authentication. . . . 79
Connecting to SAP entitlement systems. . . . 80
Setting SAP Authentication options. . . . 82
Importing SAP roles. . . . 85
Workflow for integrating with Secure Network Communication 88
5.6 Oracle EBS authentication. . . . 90
Oracle EBS Authentication. . . . 90
Enabling Oracle EBS authentication. . . . 90
Mapping Oracle E-Business Suite roles to the BI platform. . . . 91
Updating Oracle EBS roles and users. . . . 94
5.7 JD Edwards Enterprise One authentication. . . . 96
JD Edwards EnterpriseOne Authentication. . . . 96
Enabling JD Edwards EnterpriseOne authentication. . . . 96
Mapping JD Edwards EnterpriseOne roles to the BI Platform. . . . 97
5.8 PeopleSoft Enterprise authentication. . . . 101
PeopleSoft Enterprise Authentication. . . . 101
Enabling PeopleSoft Enterprise authentication. . . . 102
Mapping PeopleSoft roles to the BI Platform. . . . 103
5.9 Siebel authentication. . . . 107
Siebel Authentication. . . . 107
Enabling Siebel authentication. . . . 108
Mapping roles to the BI platform. . . . 109
5.10 X.509 Authentication. . . . 113
X.509 Authentication for BI Launch Pad. . . . 113
X.509 Authentication for Web Services. . . . 121
X.509 Authentication for CMC. . . . 124

6 Managing User Attributes. . . . 126
6.1 Managing attributes for system users 126
6.2 Prioritizing user attributes across multiple authentication options. . . . 127
6.3 To add a new user attribute. . . . 127
6.4 To edit customized user attributes. . . . 128

7 Multitenancy. . . . 130
7.1 Managing tenants in the CMC. . . . 130
To set tenant properties 130
To assign access rights to a tenant user group 132
Managing user groups for a tenant. . . . 133
To delete a tenant. . . . 134

8 Managing License. . . . 136
8.1 Managing license keys. . . . 136

To view license information. . . . 136
To add a license key. . . . 136
To view current account activity. . . . 137

9 Managing Servers. . . . 138
9.1 Working with the Servers management area in the CMC. . . . 138
9.2 To view a server's status. . . . 141
9.3 To start, stop, or restart servers with the CMC. . . . 141
9.4 To automatically start a server. . . . 141
9.5 To enable and disable servers with the CMC. . . . 142
9.6 Adding a server. . . . 142
9.7 To clone a server. . . . 143
9.8 Deleting a server. . . . 143
9.9 Add Custom Internet Headers. . . . 143
9.10 To create a non-exclusive server group. . . . 144
9.11 To add subgroups to a server group. . . . 145
9.12 To make one server group a member of another. . . . 145
9.13 Understanding Server Group Rights Management. . . . 146
9.14 To modify a server's group membership. . . . 151
9.15 To change a server's properties. . . . 152
9.16 To set a configuration template. . . . 152
9.17 To apply a configuration template to a server. . . . 153
9.18 To restore system defaults. . . . 153
9.19 To view server metrics. . . . 154
9.20 To view system metrics. . . . 154
9.21 To enable or disable destinations for a job server. . . . 154
9.22 To view server placeholders. . . . 155
9.23 To view and edit the placeholders for a node. . . . 155
9.24 To set the destination properties for a job server. . . . 156
Inbox destination properties. . . . 156
Email destination properties. . . . 157
FTP destination properties. . . . 158
SFTP destination properties. . . . 159
File System destination properties. . . . 160
9.25 Configuring Adaptive Processing Servers for production systems. . . . 161

10 Managing Web Application Container Servers (WACS). . . . 162
10.1 Web Application Container Server (WACS). . . . 162
10.2 Adding or removing additional WACS to your deployment. . . . 162
Installing WACS. . . . 163
Adding a new Web Application Container Server. . . . 163
Cloning a Web Application Container Server 164

Deleting WACS from your deployment. . . . 165
10.3 Adding or removing services to WACS. . . . 165
To add a web application or web service to a WACS. . . . 165
To remove a web application or web service from a WACS. . . . 166
10.4 To configure WACS for AD Kerberos. . . . 166
10.5 To configure WACS AD Kerberos single sign-on. . . . 167
10.6 To configure HTTPS/SSL. . . . 167
10.7 WACS and your IT environment. . . . 169
Using WACS with a reverse proxy. . . . 169
To configure WACS on a multihomed machine. . . . 170
10.8 Troubleshooting. . . . 171
To view server metrics. . . . 171
To view the state of a WACS. . . . 171
Resolving port conflicts. . . . 171
To change the number of concurrent requests. . . . 172
To prevent users from connecting to WACS through HTTP. . . . 173

11 Managing Applications. . . . 174
11.1 Overview. . . . 174
11.2 General settings. . . . 175
Setting user rights on applications. . . . 175
To set the web application trace log level in the CMC. . . . 175
11.3 Application settings. . . . 176
Managing CMC tab access. . . . 176
Managing BI launch pad settings. . . . 183
Managing Fiorified BI launch pad settings. . . . 183
Managing Web Intelligence settings. . . . 185
Managing Central Management Console settings. . . . 187
Managing BI Commentary Application Settings. . . . 190
Managing Recycle Bin Settings. . . . 192
Managing alerting settings. . . . 194
Managing widgets settings. . . . 196
Managing SAP BusinessObjects Mobile settings. . . . 196
Managing Push Notifications service in SAP BusinessObjects Mobile. . . . 200
Managing Platform Search settings. . . . 200
Configuring BEx Web Integration. . . . 207
Configuring SAP HANA single sign-on. . . . 212
Managing SAP Lumira Settings. . . . 216
Managing collaboration settings. . . . 217
Managing discussion settings. . . . 221

12 Managing Data Sources and Connections. . . . 224

12.1 Managing connections. . . . 224
To delete a universe connection. . . . 224
12.2 Managing universes. . . . 225
To delete universes. . . . 225

13 Managing Hot Backups. . . . 226
13.1 Hot backups. . . . 226
To enable hot backups. . . . 227

14 Folders. . . . 228
14.1 Folders 228
Creating a folder. . . . 228
Deleting a folder. . . . 228
Copying or moving a folder. . . . 229
Limiting report instances at the folder level. . . . 229
Limiting documents in Inboxes. . . . 230

15 Categories. . . . 231
15.1 Working with categories. . . . 231
Creating a category. . . . 231
Deleting a category. . . . 231
Moving a category. . . . 231
Adding an object to a category. . . . 232
Removing or deleting objects from a category. . . . 232
Viewing a user's personal categories. . . . 232
Adding multiple objects to a category. . . . 233

16 Object Management. . . . 234
16.1 Default settings. . . . 234
16.2 Adding an object in the CMC. . . . 236
16.3 To copy an object. . . . 236
16.4 To move an object. . . . 237
16.5 To create an object shortcut. . . . 237
16.6 To delete an object. . . . 238
16.7 To search for an object or objects. . . . 238
16.8 To send an object or an instance to a destination. . . . 239
16.9 To change the properties of an object. . . . 240
16.10 To check the relationships of an object. . . . 240
16.11 To create a new hyperlink. . . . 240

17 Reports. . . . 241
17.1 Selecting refresh options for a report. . . . 241
17.2 Selecting report viewing options for a Crystal report. . . . 241

17.3 Selecting default servers for processing an object. . . . 241
17.4 Changing database settings in Crystal reports. . . . 242
17.5 Updating default parameter values for a Crystal report. . . . 243
17.6 Updating prompts for a Web Intelligence document. . . . 243
17.7 Using filters. . . . 244
17.8 Selecting a printer for Crystal reports. . . . 244
17.9 Selecting page layout options for Crystal report and PDF objects. . . . 245
17.10 Assigning a processing extension to a report. . . . 246
17.11 Showing a thumbnail image of a Crystal report's first page. . . . 246
17.12 Adding reports to the BI repository and adding hyperlinks. . . . 246
17.13 Viewing the universes for a Web Intelligence document. . . . 247
17.14 Viewing Alerts in a Crystal report. . . . 247

18 Program Objects. . . . 248
18.1 Specifying command-line arguments. . . . 248
18.2 Setting the working directory for a program object. . . . 248
18.3 Modifying the default working directory for a program object. . . . 248
18.4 Specifying the path to external or auxiliary files. . . . 249
18.5 Uploading external or auxiliary files to the File Repository Server. . . . 249
18.6 Adding an environment variable. . . . 249
18.7 Specifying required parameters for Java programs. . . . 250
18.8 Providing Java programs with access to other files. . . . 250
18.9 Specifying a user account for a program object. . . . 251

19 Object Packages. . . . 252
19.1 To create a new object package. . . . 252
19.2 To add a new object to an object package. . . . 252
19.3 To set component failure options for an object package. . . . 252

20 Scheduling. . . . 253
20.1 Scheduling an object. . . . 253
Recurrence patterns. . . . 254
Run Options for Recurrence Patterns. . . . 255
20.2 Scheduling an object to Default Enterprise Location. . . . 256
20.3 Scheduling an object to a file location. . . . 257
20.4 Scheduling an object to an FTP server 257
20.5 Scheduling an object to an SFTP server. . . . 258
20.6 Scheduling an object to email. . . . 259
Setting up SMTP over SSL. . . . 259
20.7 Scheduling an object to user BI Inboxes. . . . 260
20.8 Enabling or disabling destinations for a job server. . . . 261
20.9 Scheduling an object based on an event. . . . 261

20.10 Scheduling an object to trigger an event. . . . 262
20.11 Configuring success or failure notification for an instance. . . . 262
20.12 Setting an alert notification. . . . 263
20.13 Selecting an output file format. . . . 263
20.14 Selecting a cache format for Web Intelligence documents. . . . 264
20.15 Scheduling a report object for individual users. . . . 264
20.16 Selecting a server or server group for a scheduled object. . . . 265
20.17 Managing instances for an object. . . . 266
20.18 Instance Manager. . . . 266
20.19 Viewing an instance. . . . 267
20.20 Pausing an instance. . . . 267
20.21 Resuming a paused instance. . . . 267
20.22 Deleting an instance. . . . 268
20.23 Setting limits for instances. . . . 268
20.24 Running multiple objects now. . . . 269
20.25 To select languages for report instances . . . 269

21 Calendars. . . . 270
21.1 Creating a calendar. . . . 270
21.2 Adding dates to a calendar. . . . 270
21.3 Deleting a calendar. . . . 271

22 Events. . . . 272
22.1 About Events. . . . 272
User Notifications. . . . 273
22.2 Events and Scheduling. . . . 276
Creating a file-based event. . . . 277
Creating a schedule-based event. . . . 278
Creating a custom event. . . . 278
Triggering a custom event. . . . 279

23 Alerting. . . . 280
23.1 Locating alert source objects in the CMC. . . . 280
23.2 Enabling alerting for an event. . . . 280
23.3 Subscribing to an alert. . . . 281
23.4 Unsubscribing from an alert. . . . 281
23.5 Subscribing other users to an alert. . . . 282
23.6 Unsubscribing other users from an alert. . . . 282
23.7 Excluding users from an alert. . . . 283
23.8 Managing alerting settings for an alert source. . . . 283

24 Profiles. . . . 285
24.1 Creating a profile. . . . 285

24.2 Specifying a global profile target for a profile. . . . 285
24.3 Specifying a profile value for a user or group. . . . 285
24.4 Using variables as profile values. . . . 286

25 About BI Admin Studio. . . . 288
25.1 About Admin Cockpit. . . . 289
Admin Cockpit. . . . 289
BI on Servers. . . . 290
BI on Document Instances. . . . 291
BI on Users and Sessions. . . . 291
BI on Content Usage. . . . 292
BI on Applications. . . . 293
25.2 Monitoring. . . . 293
Dashboard. . . . 293
Graphs. . . . 296
Probes. . . . 297
Watches. . . . 308
Metrics. . . . 315
Alerts. . . . 317
Generating Reports for Monitoring data. . . . 318
25.3 Visual Difference in the promotion management tool. . . . 318
To compare objects or files using Visual Difference. . . . 319
To compare objects or files using the Version Management System. . . . 320
To schedule the comparison. . . . 321

26 Auditing. . . . 322
26.1 Overview. . . . 322
26.2 CMC Auditing page. . . . 328
Auditing Status. . . . 329
Configuring Auditing events. . . . 330
Auditing Data Store Configuration Settings. . . . 334

27 Platform Search. . . . 336
27.1 Platform Search. . . . 336
Configuring Application Properties in the CMC. . . . 336
Indexing Failure Listing. . . . 342
Setting User Security Rights. . . . 342
Scheduling an object. . . . 345

28 Working with Federation. . . . 347
28.1 Federation. . . . 347
28.2 Federation terms. . . . 348
28.3 Managing security rights. . . . 349

Rights required on the origin site. . . . 350
Rights required on the destination site. . . . 350
Federation-specific rights. . . . 351
Replicating security on an object. . . . 352
Replicating security using access levels. . . . 353
28.4 Replication types and mode options. . . . 353
One-way replication 353
Two-way replication 354
Refresh from origin or refresh from destination. . . . 354
28.5 Replicating third-party users and groups. . . . 356
28.6 Replicating universes and universe connections. . . . 357
28.7 Managing remote connections. . . . 358
Creating remote connections. . . . 358
Modifying remote connections. . . . 360
28.8 Managing replication jobs. . . . 360
Creating replication jobs. . . . 361
To schedule a replication job. . . . 362
Modifying replication jobs. . . . 363
Viewing a log after a replication job. . . . 363
28.9 Managing object cleanup. . . . 364
How to use object cleanup. . . . 364
28.10 Managing conflict detection and resolution. . . . 365
One-way replication conflict resolution. . . . 365
Two-way replication conflict resolution. . . . 367
28.11 Using Web Services in Federation. . . . 369
Session variables 370
File caching 370
Custom deployment 371
28.12 Remote scheduling and locally run instances. . . . 372
Remote scheduling. . . . 372
Locally run instances. . . . 373
Instance share. . . . 374
28.13 Importing and promoting replicated content. . . . 374
Importing replicated content. . . . 375
Importing replicated content and continuing replication 375
Promoting content from a test environment. . . . 376
Re-pointing a destination site. . . . 376
28.14 Best practices. . . . 377
Current release limitations. . . . 380
Troubleshooting error messages. . . . 381

29 Managing Replication Lists. . . . 385

29.1 Managing replication lists. . . . 385
Creating replication lists. . . . 386
Modifying Replication Lists. . . . 387

30 Publications. . . . 389
30.1 Design tasks. . . . 389
Creating a publication in the CMC. . . . 389
Opening a Publication for Editing. . . . 389
Defining General Properties for a Publication. . . . 390
Adding Source Documents. . . . 390
Selecting Enterprise recipients. . . . 391
Selecting dynamic recipients. . . . 392
Selecting a Destination for a Publication. . . . 393
Selecting a Recurrence Pattern. . . . 394
Selecting Personalized placeholders for Publication Source Documents. . . . 396
Selecting Personalized Placeholders for Email Fields. . . . 397
Embedding Content from a Dynamic Source Document in an Email. . . . 397
Adding a Publication Extension in the CMC. . . . 398
Enabling Email Notification for a Publication Job in the CMC. . . . 399
Enabling Auditing Notification for a Publication Job in the CMC. . . . 400
Selecting Events to Trigger a Publication. . . . 400
Selecting a Server Group for a Publication. . . . 400
Selecting a Profile Resolution Method in the CMC. . . . 401
Selecting a Report Bursting Method in the CMC. . . . 401
30.2 Crystal report design tasks. . . . 401
Personalizing a Crystal Report Using Parameter Values. . . . 401
Personalizing a Crystal Report by Filtering Fields. . . . 402
Selecting the Publication Format(s) for a Crystal report. . . . 403
(Optional) Selecting Print Options for a Crystal Report in a Publication. . . . 409
(Optional) Selecting a Recipient Delivery Rule for a Crystal Report in Publication. . . . 410
(Optional) Selecting a Global Delivery Rule for a Publication. . . . 410
(Optional) Formatting a merged PDF file from Crystal reports. . . . 411
Configuring Database Logon Information for a Crystal Report in Publication. . . . 412
30.3 Web Intelligence document design tasks. . . . 413
Selecting the Publication Format for a Web Intelligence Document. . . . 413
Personalizing a Web Intelligence Document with a Global Profile Target. . . . 413
Personalizing a Web Intelligence Document by Filtering Fields. . . . 414
Editing Parameter (prompt) Values for an Object. . . . 414
30.4 Post-design tasks. . . . 415
Testing a Publication. . . . 415
Scheduling a Publication to Run. . . . 416
Subscribing or Unsubscribing from a Publication. . . . 417

Subscribing or Unsubscribing from a Publication Instance. . . . 418
Redistributing a Publication Instance. . . . 418
Retrying a Failed Publication. . . . 419

31 Rights Appendix. . . . 420
31.1 About the rights appendix. . . . 420
31.2 General rights. . . . 420
Destination Rights. . . . 423
31.3 Rights for specific object types. . . . 424
Folder rights. . . . 424
Categories. . . . 424
Crystal reports. . . . 425
Web Intelligence documents. . . . 426
Users and groups. . . . 426
Access levels. . . . 428
Universe (.unv) rights. . . . 428
Universe (.unx) rights. . . . 429
Universe object-access levels. . . . 431
Connection rights. . . . 432
Applications. . . . 433

32 Server Properties Appendix. . . . 441
32.1 About the server properties appendix. . . . 441
Common Server Properties. . . . 441
Core Services properties. . . . 443
Connectivity Services Properties. . . . 453
Crystal Reports Services Properties. . . . 457
Analysis Services Properties. . . . 465
Data Federation Services Properties. . . . 466
Web Intelligence Services properties. . . . 467

33 Server Metrics Appendix. . . . 475
33.1 About the Server Metrics Appendix. . . . 475
Common Server Metrics 476
Central Management Server Metrics. . . . 477
Connection Server Metrics. . . . 480
Event Server Metrics. . . . 481
File Repository Server Metrics. . . . 481
Adaptive Processing Server Metrics. . . . 482
Web Application Container Server Metrics. . . . 486
Adaptive Job Server Metrics. . . . 487
Crystal Reports Server Metrics. . . . 488

Web Intelligence Server Metrics. 491

34 Server Placeholders. 493

34.1 Server and node placeholders. 493

35 Managing Cryptography Keys. 502

35.1 Managing cryptographic keys in the CMC. 502

Cryptographic key status 502

To view objects associated with a cryptographic key. 503

35.2 To create a new cryptographic key. 504

35.3 To delete a cryptographic key from the system. 504

35.4 To revoke a cryptographic key. 505

35.5 To mark cryptographic keys as compromised 505

36 Promotion Management. 507

36.1 Promotion Management. 507

Welcome to promotion management. 507

Getting started with the promotion management tool. 509

Using the promotion management tool. 518

Promoting full repository content using the promotion management tool. 536

Full system promotion steps. 539

Using the Command Line option. 543

Using the Enhanced Change and Transport System. 568

Using the Promotion Management Wizard 578

36.2 Version Management. 591

To manage different versions of BI resources 591

To use Apache Subversion as the Version Management System. 592

To compare different versions of the same job. 593

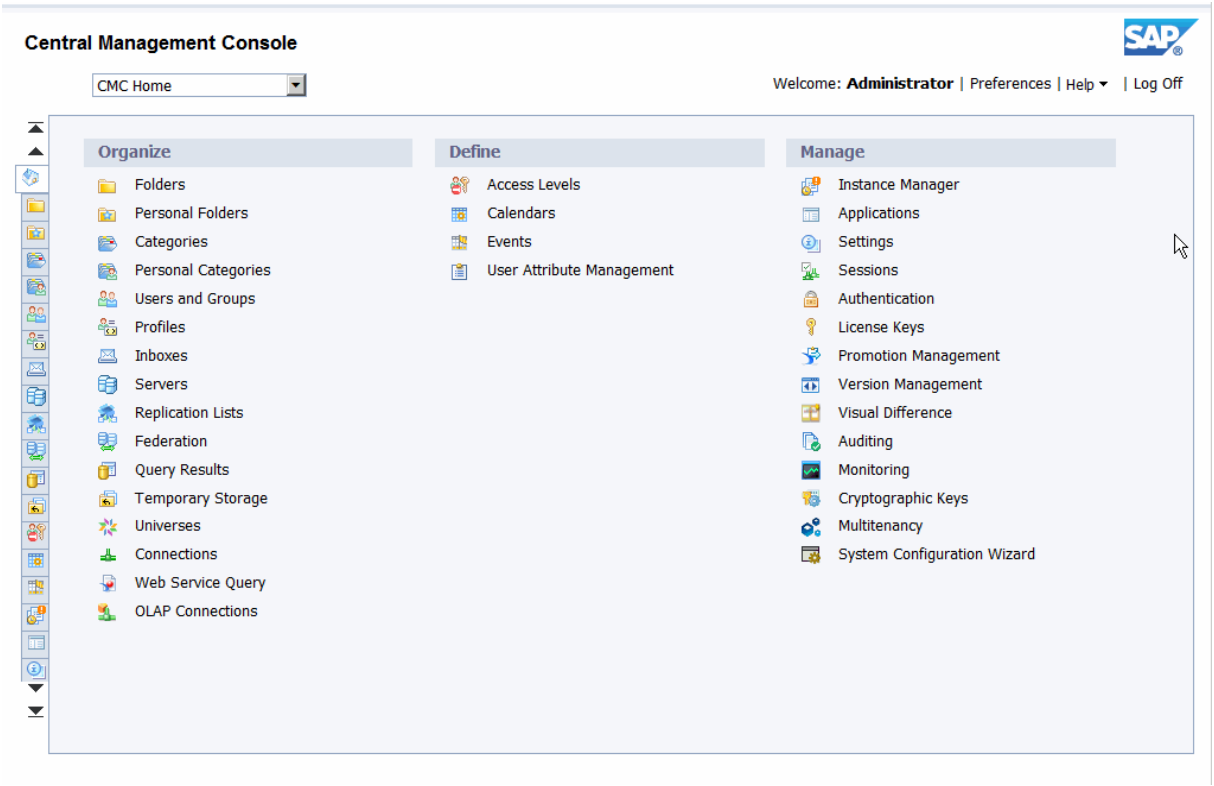
To upgrade Subversion content. 593

1 The Central Management Console

1.1 About the Central Management Console

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

Any user with valid credentials for the Business Intelligence (BI) platform can log on to the CMC and set preferences. Users who are not members of the Administrators group cannot perform management tasks, unless they have been granted access rights for a task.



There are two ways to access the CMC—from your browser or by selecting *Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *SAP BusinessObjects BI platform Central Management Console* in Windows.

1.2 Logging on to the CMC

You can log on to only one session of the Central Management Console (CMC). (You cannot run multiple sessions of the CMC on separate browser tabs or windows.)

1. In a browser, enter the URL to the CMC.

   The default URL is `http://<WebServer>:8080/BOE/CMC/`. However, your deployment may have a custom URL configured.

   Replace `<WebServer>` with the name of the web server machine. If the default virtual directory on the web server was changed, enter that URL. If necessary, change the default port number to the number provided during installation.
2. In the *System* box, enter the name of your Central Management Server (CMS).
3. If this is the first time an administrator in your organization is accessing the CMC, enter **`Administrator`** as the user name and enter the default password that was created during installation.

   After the first time, enter your user name and password.

   If you are using LDAP authentication, you can log on using an account that has been mapped to the Administrator group.
4. In the *Authentication* list, select *Enterprise*.

   Windows AD, LDAP, and other authentication methods appear in the list. However, third-party user accounts and groups must be mapped to the BI platform before you can use them.
5. Click *Log On*.

The CMC starts and the *CMC Home* window appears.

> **i** Note
>
> The User session is released once the user closes the browser.

In the future, on Windows, select *Start* > *All Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *SAP BusinessObjects BI platform Central Management Console* to start the CMC. If your CMC is hosted on a Web Application Container Server (WACS), select *Start* > *All Programs* > *SAP Business Intelligence* > *SAP BusinessObjects BI platform 4* > *SAP BusinessObjects BI platform WACS Central Management Console*.

1.3 Navigating the CMC

You can navigate the Central Management Console (CMC) in two ways.

- Click icons on the left side of the window, or click links under *Organize*, *Define*, or *Manage*.
- Select options in the *CMC Home* list in the upper-left corner of the window.

In the *tree* view, when you navigate to selections that have many child objects, not all child objects may appear. Use the paginated object listing to locate child objects.

1.4 Setting CMC preferences

Use the *Preferences* area of Central Management Console (CMC) to customize the administrative view of the BI platform. Preferences set in the CMC affect the behavior of objects in both the CMC and the BI Launch pad.

CMC preferences are applied to the platform and to the launch pad by default. However, users can set personal preferences in the BI Launch pad that override CMC preferences, until the BI platform is updated with a new software version or patch. Any platform updates reset all preferences to the default CMC settings.

If a user belongs to two or more user groups in the BI platform, the BI Launch pad displays the preferences configured for only one group.

1. Log on to the CMC, and click *Preferences* in the upper-right corner of the CMC window.
2. In the *Preferences* dialog box, set preference options as required, and click *Save & Close*.

2 System Configuration Wizard

2.1 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.

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

> **i** 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.

> **i** 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.

2.2 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.
- Whenever a product is selected or deselected, all servers that host services belonging to the Core service category in the BI platform (except services hosted by WACS) will be automatically started. The WACS will remain in its current state.
- 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.

> **i 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.

> **i 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.

> **i 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.

2.3 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: http://www.sap.com/bisizing.

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.

2.4 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.

> **i** 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

2.5 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 23]

2.6 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 24]

2.6.1 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
# Analysis edition for OLAP
Products.olap = 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.

3 Managing Users and Groups

3.1 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.

> **i** 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.

3.1.1 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.

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.
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.

     > **i** 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.

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

3.1.2 To modify a user account

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.

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 44]

3.1.3 To delete a user account

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.

> **i 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.

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 29]
To disable an alias [page 45]

3.1.4 To create a new group

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*.

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.

3.1.5 To modify a group's properties

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

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

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*.

3.1.6 To view group members

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

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.

   > **i 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.

3.1.7 To add subgroups

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

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

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 32]

3.1.8 To specify group membership

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.

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.

3.1.9 To add users or user groups in bulk

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.

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*.

The users or user groups are imported to the CMC.

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

3.1.10 To delete a group

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.

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.

3.1.11 To enable the Guest account

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.

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*.

3.1.12 To add the Customization tab to a user group

You must have "Edit objects" right in order to modify a user group.

You can add a *Customization* tab to the CMC for an application (such as Web Intelligence or BI launch pad) for a particular user group.

1. Go to the *Users and Groups* management area of the CMC.
2. Click *Group List* on the navigation panel, and right-click a user group and select *Customization*.
3. In the *Customization* dialog box, under *Customization* on the navigation panel, click the application for which to add the tab.
4. Click *Save & Close*.

3.1.13 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 32]

3.1.13.1 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.

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

> **i 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*.

3.1.13.2 Adding one or more users to a user group

You can add multiple users to a user group.

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.

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*.

3.1.14 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.

3.1.14.1 To change user password settings

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*.

> **i** 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.

3.1.14.2 To change general password settings

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	Minimum	Recommended Maximum
Must contain at least N Characters	0 characters	64 characters
Must change password every N day(s)	2 days	100 days

Password setting	Minimum	Recommended Maximum
Cannot reuse the N most recent password(s)	1 password	100 passwords
Must wait N minute(s) to change password	0 minutes	100 minutes
Disable account after N failed attempts to log on	1 failed	100 failed
Reset failed logon count after N minute(s)	1 minute	100 minutes
Re-enable account after N minute(s)	0 minutes	100 minutes

> **i 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.

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

4. Click *Update*.

Inactive user accounts will not be automatically de-activated.

3.1.15 Enabling Trusted Authentication

> **i Note**
>
> Trusted Authentication is supported for BI launch pad only; it is unavailable for the CMC.

Users prefer to log on to the system once, without needing to provide passwords several times during a session. Trusted Authentication provides a single sign-on solution for integrating your BI platform authentication solution with third-party authentication solutions. Applications that have established trust with the CMS 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.

3.1.15.1 To configure the server to use Trusted Authentication

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.

   > **i** 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.

   > **i** Note
   >
   > The time-out value determines how long the CMS waits for the IEnterpriseSession.logon() call from the client application.

6. Click *Update*.

3.1.15.2 To configure the client to use Trusted Authentication

1. Create a valid configuration file on the client machine.

   The following conditions apply for the configuration file:

   - The name of the file must be `TrustedPrincipal.conf`.
   - The file must be located at `businessobjects_root/win32_x86/`.
   - The file must contain `SharedSecret=<secretPassword>`, where `<secretPassword>` is the trusted authentication password.

2. Use the session manager to create a trusted principal and log on to the CMS:

```
ISessionMgr sessionMgr = CrystalEnterprise.getSessionMgr();
ITrustedPrincipal trustedPrincipal =
sessionMgr.createTrustedPrincipal("userName", "cmsName");
IEnterpriseSession enterpriseSession = sessionMgr.logon(trustedPrincipal);
```

3.1.16 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 48]

3.1.17 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 47]

3.1.18 Setting BI launch pad preferences for user groups in the CMC

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

Administrators can specify default values for the following BI launch pad preferences in the CMC:

- *Home* tab
- Location where documents are stored
- Folders
- Categories
- Number of objects per page
- Columns displayed on the *Document* tab
- Whether to display documents in BI launch pad on a tab or in a new window

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

Users can configure their own preferences in BI launch pad, and the preference values take precedence over the default values. (Users can switch back to the default preferences at any time.) However, if the administrator modifies the default BI launch pad preferences in the CMC, the default values take precedence over the user-defined values.

3.1.18.1 Setting BI launch pad preferences for a user group

BI launch pad preferences configured in the CMC are the default preferences for all users in a user group.

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

Users can define their own BI launch pad preferences, if they have appropriate access rights. If you do not want users to modify preferences, do not grant users the right to set preferences.

1. Go to the *Users and Groups* management area of the CMC.
2. Under *Group List*, select the user group for which to set BI launch pad preferences.
3. Select *Actions* > *BI launch pad Preferences*
   The *BI Launch Pad Preferences* dialog box appears.
4. Clear the *No Preferences Defined* check box.
5. Select either *Home tab* or *Documents tab* to choose the default start page in BI launch pad.
6. If you selected *Home tab*, perform one of the following actions to choose the home page on the tab:
   - To display the default BI launch pad *Home* tab, select *Default Home tab*.
   - To display a specific web site as the *Home* tab, select *Select Home tab*, click *Browse Home Tab*, select an object in the BI repository, and click *Open*.
7. If you selected *Documents tab*, perform one of the following actions:
   - Select *My Documents* to display your documents drawer, and select the default node to display:
     - *My Favorites*
     - *Personal Categories*
     - *My Inbox*
   - Select *Folders* to display your folders drawer, and select the default folder to display:
     - To choose all public folders, select *Public Folders*.
     - To choose a particular folder, select *Select Public folder*, click *Browse Folder*, select the folder, and click *Open*.
   - Select *Categories* to display your categories drawer, and select the default category to display:
     - To choose all public categories, select *Corporate Categories*.
     - To choose a particular category, select *Select Corporate Category*, click *Browse Category*, select the category, and click *Open*.
8. Under *Choose Columns to Display on Documents Tab*, select the check box for each column to display for each object in the *List* panel:
   - *Type*
   - *Last Run*
   - *Instances*
   - *Description*
   - *Created By*
   - *Created On*
   - *Location (Categories)*

- *Received On (Inbox)*
- *From (Inbox)*

9. Under *Set document viewing location*, perform one of the following actions choose how users will view documents:
   - Select *In the BI launch pad portal as tabs* to display documents on individual tabs in BI launch pad.
   - Select *In multiple full screen browser windows, one window for each document* to display documents in individual browser windows.
10. In the *Set the maximum number of items per page* box, enter the maximum number of objects to display per BI launch pad page when a user views lists of objects.
11. Click *Save & Close*.

3.1.19 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.

3.1.19.1 Setting Fiorified BI Launch pad preferences for a user group

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*

Home page tab option	Action
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)*

> **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*.

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*.

3.2 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.

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

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.

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.

3.2.2 To create a new alias for an existing user

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.

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.

3.2.3 To assign an alias from another user

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.

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*.

3.2.4 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.

> ℹ 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.

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.

3.2.5 To disable an alias

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.

> ℹ 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.

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 45]

4 Setting Rights

4.1 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.

4.1.1 To view rights for a principal on an object

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

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.

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

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.

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.

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 48]

4.1.3 To modify security for a principal on an object

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.

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 48]

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

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

> **i** 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.

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 48]
To modify security for a principal on an object [page 48]

4.1.5 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.

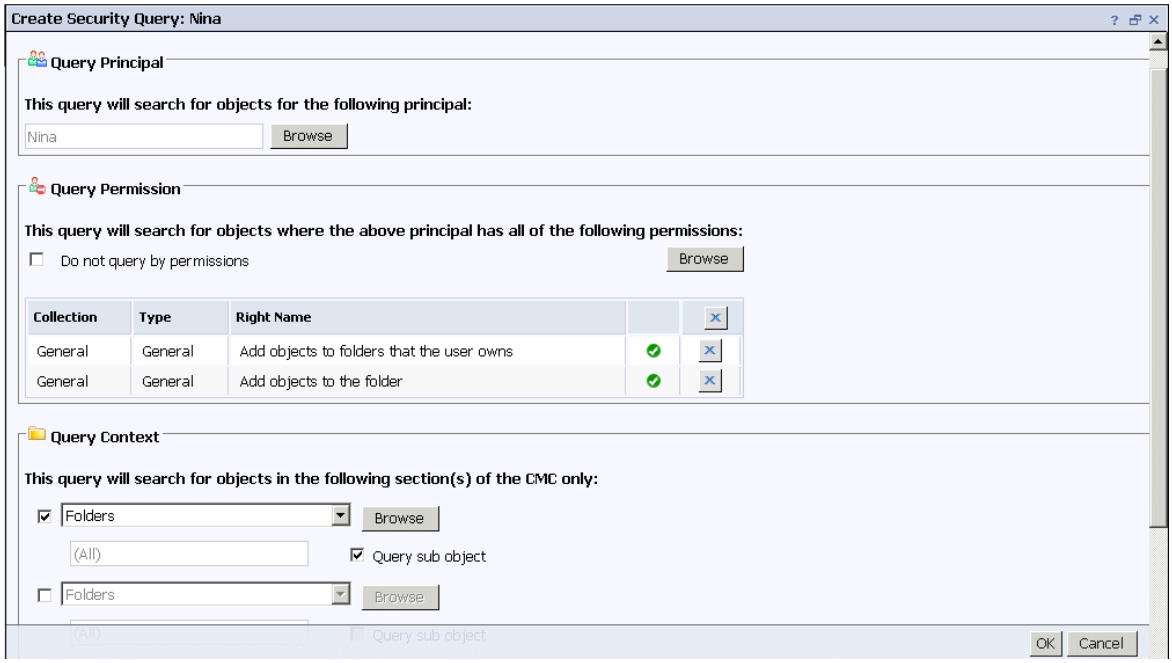
- Query context
  You specify the CMC areas that you want the security query to search. For each area, you can choose whether to include sub-objects in the security query. A security query can have a maximum of four areas.

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.

4.1.5.1 To run a security query

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.

      > ℹ 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.

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.

4.2 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

Access level task	Rights required
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 **i 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

4.2.1 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.

4.2.2 To copy an existing access level

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.

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.

4.2.3 To create a new access level

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.

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.

4.2.4 To rename an access level

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.

4.2.5 To delete an access level

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*.

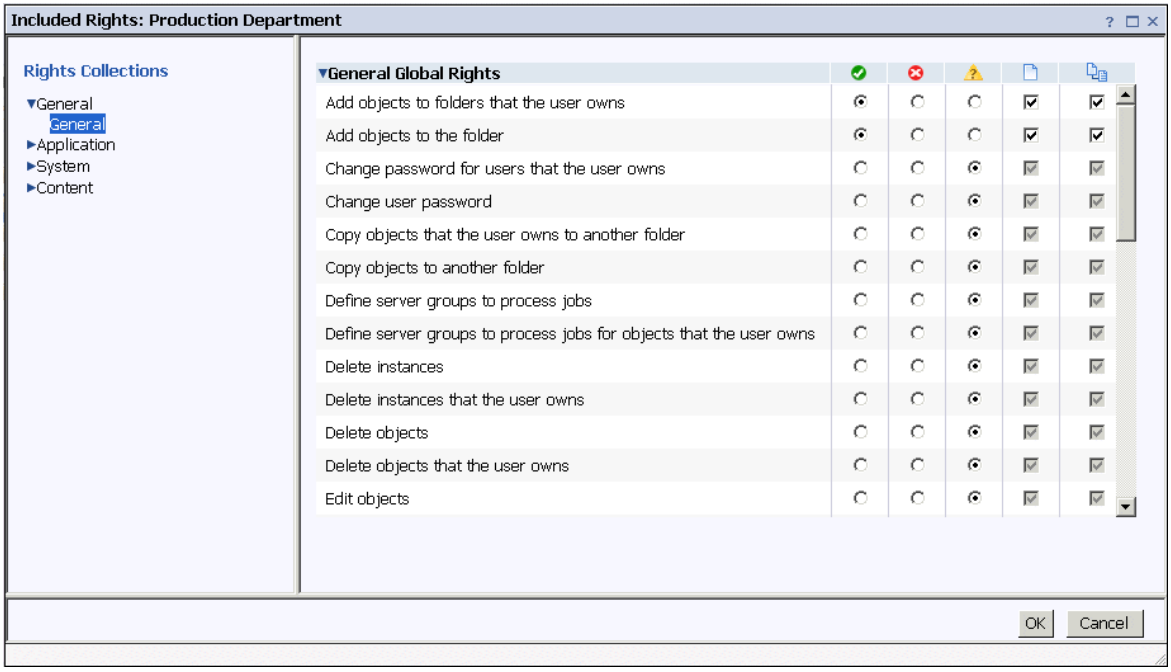
   > **i** Note
   >
   > You cannot delete predefined access levels.

   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.

4.2.6 To modify rights in an access level

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.

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.

4.2.7 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.

4.2.8 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

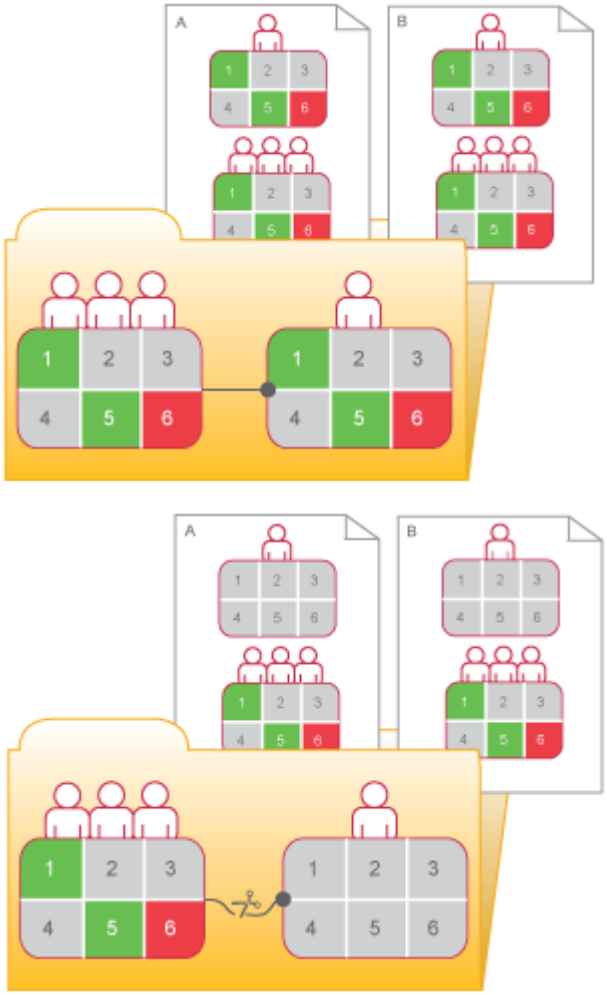
Federation [page 347]
Tracing the relationship between access levels and objects [page 56]

4.3 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.

> **i** 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

4.3.1 To disable inheritance

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

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*.

5 Authentication

5.1 Overview

5.1.1 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
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Because the BI platform is fully customizable, the authentication and processes may vary from system to system.

5.2 Enterprise authentication

5.2.1 Enterprise authentication

Enterprise authentication is the default authentication method for the BI platform; it is automatically enabled when you first install the system, and it cannot be disabled. When you add and manage users and groups, the platform maintains the user and group information within its database. 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.

Related Information

Enterprise authentication settings [page 61]
To change Enterprise settings [page 62]
To change general password settings [page 62]

5.2.2 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. **i 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.
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.
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.

Settings	Options	Description
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.

5.2.2.1 To change Enterprise settings

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.

5.2.2.2 To change general password settings

> ℹ Note
>
> Accounts not used for an extended period of time are not automatically de-activated. Administrators must manually delete inactive accounts.

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	Minimum	Recommended Maximum
Must contain at least N Characters	0 characters	64 characters
Must change password every N day(s)	2 days	100 days
Cannot reuse the N most recent password(s)	1 password	100 passwords

Password setting	Minimum	Recommended Maximum
Must wait N minute(s) to change password	0 minutes	100 minutes
Disable account after N failed attempts to log on	1 failed	100 failed
Reset failed logon count after N minute(s)	1 minute	100 minutes
Re-enable account after N minute(s)	0 minutes	100 minutes

4. Click *Update*.

5.3 LDAP authentication

5.3.1 LDAP authentication

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 accounts to the BI platform. When you map an LDAP account, you can choose to create a new account or link to an existing Enterprise 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.

The LDAP Configuration Wizard is provided to help administrators perform the following tasks:

- Configuring the LDAP host
- Preparing the LDAP server for SSL (if required)
- Configuring the LDAP plug-in for SiteMInder (if required)

The SAP authentication application is used to configure how users authenticate into the BI platform.

> **i** 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.

Related Information

To configure the LDAP host [page 64]
Mapping LDAP groups [page 71]

Configuring SSL settings for LDAP Server or Mutual Authentication [page 66]
Configuring the LDAP plug-in for SiteMinder [page 70]

5.3.1.1 To configure the LDAP host

It is recommended that your LDAP server be installed and running before configuring the LDAP host.

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.

   > ℹ 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 66]
Configuring the LDAP plug-in for SiteMinder [page 70]

5.3.2 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 64]

5.3.2.1 To configure the LDAP Server or Mutual Authentication

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.

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.

Resource	Take this action before starting this task
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>`.
	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`

Resource	Take this action before starting this task

	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.

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 70]

5.3.3 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 64]

5.3.3.1 To configure LDAP for single sign-on with SiteMinder

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.

5.3.4 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.

5.3.4.1 To map LDAP groups using the BI platform

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*.

5.3.4.2 To unmap LDAP groups using the BI platform

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.

> **i** 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.

To deny LDAP Authentication for all groups, clear the "LDAP Authentication is enabled" check box and click *Update*.

5.4 Windows AD authentication

5.4.1 Windows AD authentication

The BI platform supports Windows AD authentication for user and group accounts. Before users can use their Windows AD user name and password to log on to the system, you need to map their accounts to the BI platform.

Basic Windows AD authentication workflow

To set up AD authentication with the BI platform you must follow the following workflow:

1. Enable the Windows AD security plug-in and map in users and groups.
2. Choose an authentication method:
   - Windows AD with Kerberos
   - Windows AD with NTLM
3. Set up single sign-on to BI platform applications. This optional step can be facilitated via the following methods:
   - Windows AD with Kerberos
   - Windows AD with NTLM
   - Windows AD with SiteMinder

5.4.2 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.

  > **i** 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.

5.4.3 To configure Windows AD authentication

Regardless of which protocol (Kerberos or NTLM) is used, you must complete the following steps to allow AD users to authenticate. These steps include instructions for mapping Windows AD users and groups, and to schedule updates. The procedure below does not include steps for configuring Windows AD with SiteMinder.

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Ensure that *Enable Windows Active Directory (AD)* box is selected.
4. In the *Windows AD Configuration Summary* area, click the link beside *AD Administration Name*.

   > **i** Note
   >
   > Before the Windows AD plug-in is configured, this link will appear as two double quotes. After the configuration has been saved, the link with be populated with the AD Administration names.

5. Enter the name and password of an enabled domain user account. The BI platform will use this account to query information from AD.

   Administration credentials can use one of the following formats:

   - NT name (`DomainName\UserName`)
   - UPN (`user@DNS_domain_name`)

   The BI platform never modifies, adds or deletes content from AD. It only reads information; therefore only the appropriate rights are required.

   > **i** Note
   >
   > AD authentication will not continue if the AD account used to read the AD directory becomes invalid (for example, if the account's password is changed or expires or the account is disabled).

6. Complete the *Default AD Domain* field.

   > **i** Note
   >
   > - Groups from the default domain can be mapped without specifying the domain name prefix.
   > - If you enter the Default AD Domain name, users from the default domain do not have to specify the AD domain name when they log on to the BI platform via AD authentication.

7. In the *Mapped AD Member Groups* area, enter the AD domain\group in the *Add AD Group (Domain\Group)* field.

   Groups can be mapped using one of the following formats:

   - Security Account Manager account name (SAM), also referred to as NT name (`DomainName\GroupName`)
   - DN (`cn=GroupName, ......, dc=DomainName, dc=com`)

   > **i Note**
   >
   > If you want to map a local group, you can use only the NT name format (\\ServerName\GroupName). Windows AD does not support local users. This means that local users who belong to a mapped local group will not be mapped to the BI platform. Therefore, they will not be able to access the system.

8. Click *Add*.

   The group is added to the list.

9. Select one of the following under *Authentication Options*:

   - Use NTLM authentication
   - Use Kerberos authentication

   If you select Kerberos, you need to select Cache security context if you plan to configure single sign-on to the database. Kerberos authentication configuration involves resources beyond the scope of the CMC. For detailed information on setting up Windows AD authentication with Kerberos see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

   > **i Note**
   >
   > To configure the BI platform for Kerberos and Windows AD 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 platform servers. In the *Service principal name* field, enter the account and domain of the service account or the SPN mapping to the service account. Use the following format, where **`svcacct`** is the name of the service account or SPN you created earlier, and **`DNS.COM`** is your fully qualified domain in uppercase.

10. If you plan to set up single sign-on for the Windows AD users and groups, select *Enable Single Sign On for selected authentication mode*.
11. Select the option in the *Synchronization of Credentials* area to enable and update the Windows AD user's data source credentials at logon time. This will synchronize the data source with the user's current logon credentials
12. In the *AD Alias Options* area specify how new aliases are added and updated to the BI platform.
    a. In *New Alias Options*, select how new aliases are mapped to Enterprise accounts. Select one of the following choices:
       - *Assign each new AD alias to an existing User Account with the same name*
         Use 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*
         Use this option when you want to create a new account for each user.

b. In *Alias Update Options*, select how to manage alias updates for the Enterprise accounts. Select one of the following choices:

- *Create new aliases when the Alias Update occurs*
  Use this option to automatically create a new alias for every 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 the "Create a new account for each new AD alias" option and clicked *Update*
- *Create new aliases only when the user logs on*
  Use this option when the AD 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 *New User Options* specify how new users are created by selecting one of the following choices:

- *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.
- *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.

13. To configure how to schedule AD alias updates, click *Schedule AD Alias Updates*.
    a. In the *Schedule* dialog box, select a recurrence from the *Run object* drop-down list.
    b. Set any of the other schedule options and parameters as required.
    c. Click *Schedule*.
    When the alias update occurs, the group graph is also updated.
14. In the *Attribute Binding Options* area you can select the following optional settings:

- *Import Full Name and Email Address*
  If selected, the AD user account full names and descriptions are imported and stored with the user object in the BI platform.
- *Give AD attribute binding priority over LDAP attribute binding*
  If selected, AD attributes take priority in scenarios where both Windows AD and LDAP are enabled.

15. You can configure AD group graph updates in the *AD Group Options* area.
    a. Click *Schedule AD Group Updates*.
    The *Schedule* dialog box appears.
    b. Select a recurrence from the *Run object* drop-down list.
    c. Set any of the other schedule options and parameters as required.
    d. Click *Schedule*.

    The system will schedule the update and run it according to the schedule information you specified. You can view the next scheduled update for the AD group accounts under the *AD Group Graph Options*.
16. Use the settings in the *On-demand AD Update* area to specify what should be updated. You can select from one of the following options:

- *Update AD Groups now*

Select this option if you want to update the group graph. The update will occur only after you click *Update*.

> **i Note**
>
> This option affects any scheduled group graph updates. The next scheduled group graph update is listed under *AD Group Graph Options*.

- *Update AD Groups and Aliases now*
  Select this option if you want to update the group graph and user aliases. The updates will occur only after you click *Update*.

  > **i Note**
  >
  > This option affects any scheduled group graph or updates. The next scheduled updates are listed under *AD Group Graph Options* and *AD Alias Options*.

- *Do not update AD Groups and Aliases now*
  If you click *Update*, neither the group nor the user aliases will be updated.

  > **i Note**
  >
  > This option affects any scheduled group or alias updates. The next scheduled updates are listed under *AD Group Options* and *AD Alias Options*.

17. Click *Update*.
18. Click *OK*.

5.4.4 To map Windows AD groups

Windows AD authentication should be enabled before you import groups.

The Window AD authentication application is used for both configuring authentication and mapping Windows AD groups. Use the procedure below to map your Windows AD groups.

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Ensure that *Enable Windows Active Directory (AD)* box is selected.
4. In the *Windows AD Configuration Summary* area, click the link beside *AD Administration Name*.
5. Enter the name and password of an enabled domain user account. The system will use this account to query information from AD.

   Administration credentials can use one of the following formats:

   - NT name (`DomainName\UserName`)
   - UPN (`user@DNS_domain_name`)

   The BI platform never modifies, adds or deletes content from AD. It only reads information; therefore only the appropriate rights are required.

> **Note**
>
> AD authentication will not continue if the AD account used to read the AD directory becomes invalid (for example, if the account's password is changed or expires or the account is disabled).

6. Complete the *Default AD Domain* field.

> **Note**
>
> - Groups from the default domain can be mapped without specifying the domain name prefix.
> - If you enter the Default AD Domain name, users from the default domain do not have to specify the AD domain name when they log on to the BI platform via AD authentication.

7. In the *Mapped AD Member Groups* area, enter the AD domain\group in the *Add AD Group (Domain\Group)* field.

   Groups can be mapped using one of the following formats:

   - 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, you can use only the NT name format (\\ServerName\GroupName). Windows AD does not support local users. This means that local users who belong to a mapped local group will not be mapped to the BI platform. Therefore, they will not be able to access the system.

8. Click *Add*.
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. Click *Update*.
11. Click *OK*.

5.5 SAP authentication

5.5.1 SAP Authentication

SAP authentication enables SAP users to log on to the BI platform using their SAP user names and passwords, without having to store these passwords in the BI platform system. SAP authentication also allows you to preserve information about user roles in SAP, and to use this role information within the BI platform to assign rights to perform administrative tasks, or access content.

The SAP authentication application is used to configure how users authenticate into the BI platform and to import and update roles from your SAP system.

The application is divided into four tabs described in the table below.

Tab	Description
Entitlement Systems	Contains the settings to identify the SAP system that will be integrated with the BI platform.
Role Import	Contains settings to identify which roles to import into the BI platform.
SNC Settings	Contains settings for configuring Secure Network Communication (SNC) between the target SAP system and the BI platform.
Options	Contains the setting for enabling SAP authentication. This tab also has settings for : • Connection options • How users are imported into the BI platform system • Importing key files for setting up the SAP single sign-on (SSO) service
User Update	Contains the settings for scheduling and running updates for imported SAP roles.

Related Information

Connecting to SAP entitlement systems [page 80]
Setting SAP Authentication options [page 82]
Importing SAP roles [page 85]
Updating SAP roles and users [page 87]
To configure SNC settings in the Central Management Console [page 89]

5.5.2 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.

5.5.2.1 To add an SAP entitlement system

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.

   > **i** 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.

   > **i** 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.

   > **i** Note
   >
   > These credentials must correspond to the user account that you created for the BI platform.

9. Click *Update*.

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).

5.5.2.2 To verify if your entitlement system was added correctly

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.

5.5.3 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

5.5.3.1 To set SAP Authentication options

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. **i 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. **i 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.

Setting	Description
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. **i 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. 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.

Setting	Description
	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. **i 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. **i 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.

Setting	Description
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*.

5.5.3.2 To change the Content folder root

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/`).

5.5.4 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.

> **i 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.

> **i 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.

5.5.4.1 To import SAP roles

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*.

5.5.4.2 To verify that roles and users were imported correctly

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.

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.

5.5.4.3 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.

5.5.4.3.1 To schedule updates for SAP roles

After you map roles in the BI platform, you must specify how the system updates the roles.

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.

5.5.5 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 85]

5.5.5.1 To configure SNC settings in the Central Management Console

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.

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*.

   > **i 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 80]

5.6 Oracle EBS authentication

5.6.1 Oracle EBS Authentication

Oracle EBS authentication enables users to log on to the BI platform using their EBS user names and passwords, without having to store these passwords in the system.

The Oracle EBS authentication application is used to configure how users authenticate into the BI platform and to import roles from your EBS system.

The application is divided into four tabs described in the table below.

Tab	Description
Options	Contains the setting for enabling Oracle EBS authentication and options defining how to handle new aliases, alias updates, and new users.
Systems	Contains settings for the Oracle EBS system user and services to be accessed by the BI platform.
Responsibilities	Contains the settings for importing roles into the BI platform.
User Update	Contains the settings for scheduling and running updates for imported Oracle EBS roles.

Related Information

To enable Oracle E-Business Suite authentication [page 91]
To map Oracle E-Business Suite roles [page 92]
To schedule updates for Oracle EBS roles [page 95]

5.6.2 Enabling Oracle EBS authentication

To allow Oracle EBS information to be used by the BI platform, the system needs information on how to authenticate into your Oracle EBS system.

5.6.2.1 To enable Oracle E-Business Suite authentication

Prior to performing the procedure, Oracle DLL and JAR files need to be deployed on the BI platform:

1. Download `ojdbc11.dll` from the Oracle database client application.
2. Copy the file to this location:
   - Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`
   - UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/platform`
3. Download `ojdbc5.jar` from the Oracle database client application.
4. Copy the file to this location:
   - Windows: `<INSTALLDIR>\Tomcat\lib`
   - UNIX: `<INSTALLDIR>/sap_bobj/tomcat/lib`

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Click *Oracle EBS*.
   The *Oracle EBS* page appears. It has four tabs: *Options*, *Systems*, *Responsibilities*, and *User Update*.
4. On the *Options* tab, select the *Oracle EBS Authentication is enabled* 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 *Systems* tab.
6. Click the *Systems* tab.
7. In the *Oracle EBS System User* area, type a database User name and Password for the BI platform to use to log on to your Oracle E-Business Suite database.
8. In the *Oracle EBS Services* area, enter the service name used by your Oracle EBS environment and click *Add*.
9. Click *Update* to save your changes.

You now need to map Oracle EBS roles into the system.

Related Information

To map Oracle E-Business Suite roles [page 92]

5.6.3 Mapping Oracle E-Business Suite roles to the BI platform

The BI platform automatically creates a group for each Oracle E-Business Suite (EBS) role that you map. The system also creates aliases to represent the members of the mapped Oracle E-Business Suite 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 system.

For example, if you run a EBS test environment and production environment, 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 your test environment with a user account for Russell Aquino (user name "raquino"), and you run the production environment 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 on to the system with their own Oracle EBS credentials and have access to data from both EBS environments.

5.6.3.1 To map Oracle E-Business Suite roles

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Click *Oracle EBS*.
   The *Oracle EBS* page displays the *Options* tab.
4. In the *New Alias Options* area, select one of the following options:
   - *Assign each added Oracle EBS alias to an account with the same name*
     Select this option if you run multiple Oracle E-Business Suite systems with users who have accounts on more than one system (and if no two users have the same user name for different systems).
   - *Create a new account for every added Oracle EBS alias*
     Select this option if you run only one Oracle E-Business Suite, 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.
5. In the *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 BI platform accounts or for all users if you selected the *Create a new account for every added Oracle EBS 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.
6. In *New User Options* specify how new users are created, and then click *Update*.

   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 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.

7. Click the *Responsibilities* tab.
8. Under *Current Oracle EBS Services*, select the Oracle EBS service that contains the roles you want to map.
9. You can specify filters for Oracle EBS users under *Mapped Oracle EBS Roles*.
   a. Select which applications users can use for the new role from the *Application* list.
   b. Select what Oracle applications, functions, reports, and concurrent programs the user can run in the *Responsibility* list.
   c. Select which security group the new role is assigned to in the Security group in the *Security Group*
   d. Use the *Add* and *Delete* buttons under *Current Role* to modify the security group assignments for the role.
10. Click *Update*.
    The roles will be mapped to the BI platform.

After you map roles into the BI platform, you need to specify how the system updates these roles.

5.6.3.2 Adding users to mapped roles

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.

5.6.3.3 Unmapping roles

To prevent specific user groups from logging on to the BI platform, you can unmap the roles to which they belong.

5.6.3.3.1 To unmap a role

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Double-click the name of the ERP system you want to unmap roles for.
   The ERP system page displays the *Options* tab.
4. Click the *Responsibilities* tab.
5. Select the *Current Oracle EBS Service*.
6. Under *Current Role*, select a role and then click the *Delete* button.
7. Click *Update*.

   Members of the role will no longer be able to access the BI platform, unless they have other accounts or aliases.

   > **i** 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.

5.6.4 Updating Oracle EBS roles and users

After enabling Oracle EBS 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 updated Oracle EBS role information is accurately reflected in the BI platform.

There are two options for running and scheduling updates for Oracle EBS 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 Oracle EBS 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 Oracle EBS system.

> **i** Note
>
> If you have not specified to automatically create user aliases for updates when you enabled Oracle EBS authentication, no accounts will be created for new aliases.

5.6.4.1 To schedule updates for Oracle EBS roles

After you map roles into the BI platform you need to specify how the system updates these roles.

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 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* pull-down 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 at what time it will start, as well as a start and end date.
Daily	The update will run every day or 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 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.

5.7 JD Edwards Enterprise One authentication

5.7.1 JD Edwards EnterpriseOne Authentication

JD Edwards EnterpriseOne authentication enables users to log on to the BI platform using their JD Edwards user names and passwords, without having to store these passwords in the BI platform.

The JD Edwards EnterpriseOne authentication application is used to configure how users authenticate into the BI platform and to import roles from your JD Edwards system.

The application is divided into four tabs described in the table below.

Tab	Description
Options	Contains the setting for enabling JD Edwards EnterpriseOne authentication and options defining how to handle new aliases, alias updates, and new users.
Systems	Contains settings for the JD Edwards EnterpriseOne system user and services to be accessed by the BI platform.
Responsibilities	Contains the settings for importing roles into the BI platform.
User Update	Contains the settings for scheduling and running updates for imported JD Edwards EnterpriseOne roles.

Related Information

Enabling JD Edwards EnterpriseOne authentication [page 96]
Mapping JD Edwards EnterpriseOne roles to the BI Platform [page 97]
Scheduling user updates [page 100]

5.7.2 Enabling JD Edwards EnterpriseOne authentication

To allow JD Edwards EnterpriseOne information to be used by the BI platform, the platform needs information on how to authenticate into your JD Edwards EnterpriseOne system.

5.7.2.1 To enable JD Edwards authentication in the BI Platform

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Double-click *JD Edwards EnterpriseOne*.
   The *JD Edwards EnterpriseOne* page appears.
4. On the *Options* tab, select the *Enable JD Edwards EnterpriseOne 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 *Systems* tab.
6. Click the *Servers* tab.
7. Copy `jdeutil.jar`, `kernel.jar`, and `log4j.jar` from the JD Edwards installation to these locations (on Windows): `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` and `<INSTALLDIR>\Tomcat\lib\`.
8. Restart Tomcat and the Server Intelligence Agent.
9. In the *JD Edwards EnterpriseOne System User* area, type a database User name and Password for the BI platform to log on to your JD Edwards EnterpriseOne database.
10. In the *JD Edwards EnterpriseOne Domain* area, enter the name, host, and port used to connect to your JD Edwards EnterpriseOne environment.
11. Enter a name for the environment, and click *Add*.
12. Click *Update* to save your changes.

5.7.3 Mapping JD Edwards EnterpriseOne roles to the BI Platform

The BI platform automatically creates a group for each JD Edwards EnterpriseOne role that you map. As well, the system creates aliases to represent the members of the mapped JD Edwards EnterpriseOne 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 a JD Edwards EnterpriseOne test environment and production environment, 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 your test environment with a user account for Russell Aquino (user name "raquino"), and you run the production environment with a user account for Raoul Aquino (user name "raquino"), then you need to create a separate account for each user's alias. If you do not, the two users are added to the

same BI platform account, and they will not be able to log on to the BI platform with their own JD Edwards EnterpriseOne credentials.

5.7.3.1 To map a JD Edwards EnterpriseOne role

1. Log on as an administrator to the Central Management Console.
2. From the *Manage* area, click *Authentication*.
3. Double-click *JD Edwards EnterpriseOne*.
4. In the *New Alias Options* area, select one of the following options:
   - *Assign each added alias to an account with the same name*
     Select this option if you run multiple JD Edwards EnterpriseOne 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 JD Edwards EnterpriseOne, 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.
5. In the *Update Options* area, select one of the following options:
   - *New aliases will be added and new users will be created*
     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 BI platform accounts or for all users if you selected the Create a new account for every added alias option.
   - *No new aliases will be added and new users will not be created*
     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 system 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.
6. 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.

     > **i 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.

7. Click the *Roles* tab.
8. Under *Domain List*, select the JD Edwards server that contains the roles you want to map.
9. Under *Available Roles*, select the roles you want to map to the BI platform and click <.
10. Click *Update*.
    The roles will be mapped to the BI platform.

5.7.3.2 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.

5.7.3.3 Unmapping roles

To prevent users from logging on to the BI platform, you can unmap the roles to which they belong.

5.7.3.3.1 To unmap a role

1. Log on as an administrator to the Central Management Console.
2. From the *Manage* area, click *Authentication*.
3. Click the tab for *JD Edwards EnterpriseOne*.
4. In the *Roles* area, select the role that you want to remove, and click <.
5. 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.

5.7.3.4 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.

5.7.3.4.1 To schedule user updates

After you map roles into the BI platform, you need to specify how the system updates these roles.

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.

> **i** 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.

5.8 PeopleSoft Enterprise authentication

5.8.1 PeopleSoft Enterprise Authentication

PeopleSoft Enterprise authentication enables users to log on to the BI platform using their PeopleSoft user names and passwords, without having to store these passwords in the BI platform.

The PeopleSoft Enterprise authentication application is used to configure how users authenticate into the BI platform and to import roles from your PeopleSoft system.

The application is divided into four tabs described in the table below.

Tab	Description
Options	Contains the setting for enabling PeopleSoft Enterprise authentication and options defining how to handle new aliases, alias updates, and new users.
Systems	Contains settings for the PeopleSoft Enterprise system user and services to be accessed by the BI platform.
Responsibilities	Contains the settings for importing roles into the BI platform.
User Update	Contains the settings for scheduling and running updates for imported PeopleSoft Enterprise roles.

Related Information

Enabling PeopleSoft Enterprise authentication [page 102]
Mapping PeopleSoft roles to the BI Platform [page 103]
Scheduling user updates [page 100]

5.8.2 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.

5.8.2.1 To enable PeopleSoft Enterprise authentication in the BI platform

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.

5.8.3 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.

5.8.3.1 To map a PeopleSoft role to the BI Platform

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.

Main steps:

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.

5.8.3.2 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.

5.8.3.3 To unmap a role

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.

5.8.3.4 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.

5.8.3.4.1 To schedule user updates

After you map roles into the BI platform, you need to specify how the system updates these roles.

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.

> **i 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.

5.9 Siebel authentication

5.9.1 Siebel Authentication

Siebel authentication enables users to log on to the BI platform using their Siebel user names and passwords, without having to store these passwords in the BI platform.

The Siebel authentication application is used to configure how users authenticate into the BI platform and to import roles from your Siebel system.

The application is divided into four tabs described in the table below.

Tab	Description
Options	Contains the setting for enabling Siebel authentication and options defining how to handle new aliases, alias updates, and new users.
Systems	Contains settings for the Siebel system user and services to be accessed by the BI platform.
Responsibilities	Contains the settings for importing roles into the BI platform.
User Update	Contains the settings for scheduling and running updates for imported Siebel roles.

Related Information

Enabling Siebel authentication [page 108]
Mapping roles to the BI platform [page 109]
Scheduling user updates [page 100]

5.9.2 Enabling Siebel authentication

To allow Siebel information to be used by the BI platform, it needs information on how to authenticate into your Siebel system.

5.9.2.1 To enable Siebel authentication in the BI Platform

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Double-click *Siebel*.
   The *Siebel* page appears. It has four tabs: *Options*, *Systems*, *Responsibilities*, and *User Update*.
4. On the *Options* tab, select the *Enable Siebel 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 *Systems* tab.
6. Click the *Domains* tab.
7. In the *Domain Name* field enter the domain name for the Siebel system you want to connect to.
8. Under *Connection* enter the connection string for that domain.
9. In the *Username* area, type a database User name and Password for the BI platform to use to log on to your Siebel database.
10. In the *Password* area, enter the password for the user you have selected.
11. Click *Add* to add the system information to your *Current Domains* list.

12. Click *Update* to save your changes.

5.9.3 Mapping roles to the BI platform

The BI platform automatically creates a group for each Siebel role that you map. As well, the program creates aliases to represent the members of the mapped Siebel 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 program.

For example, if you run a Siebel eBusiness test environment and production environment, 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 your test environment with a user account for Russell Aquino (user name "raquino"), and you run the production environment with a user account for Raoul Aquino (user name "raquino"), then you need to create a separate account for each user's alias. If you do not, the two users are added to the same account, and they will not be able to log on to the BI platform with their own Siebel eBusiness credentials.

5.9.3.1 To map a Siebel eBusiness role to the BI Platform

1. Log on as an administrator to the Central Management Console.
2. Click *Authentication*.
3. Double-click *Siebel*.
4. Select the check box *Enable Siebel Authentication*.
5. In the *New Alias Options* area, select one of the following options:
   - *Assign each added alias to an account with the same name*
     Select this option if you run multiple Siebel eBusiness 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 Siebel eBusiness, 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.
6. 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 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 program 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.

7. In the *New User Options* area specify how new users are created.

   If your BI platform license is based on users roles, select one of the following options:

   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.

     > **i 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.

8. Click the *Roles* tab.
9. Select the domain that corresponds to the Siebel server you want to map roles for.
10. Under *Available roles*, select the roles you want to map and click >.

> **i Note**
>
> You can use the *Search Roles Begin With:* field to narrow your search if you have a large number of roles. Enter the characters that the role or roles begin with followed by the wildcard (%) character, and click *Search*.

> **i Note**
>
> For the search function to work, a Siebel plugin jar file needs to be deployed to the Tomcat lib directory: `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\lib` and to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. Then restart the Tomcat server and Server Intelligence Agent.

11. Click *Update*.
    The roles will be mapped to the BI platform.

5.9.3.2 Remapping consideration

To enforce group and user synchronization between the BI platform and Siebel, set the *Force user synchronization*.

> **i** Note
>
> In order to select *Force user synchronization* you must first select *New aliases will be added and new users will be created*.

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.

5.9.3.3 Unmapping roles

To prevent users from logging on to the BI platform, you can unmap the roles to which they belong.

5.9.3.3.1 To unmap a role

1. Log on as an administrator to the Central Management Console.
2. From the *Manage* area, click *Authentication*.
3. Double-click *Siebel*.
4. On the *Domains* tab select the Siebel domain that corresponds to the role or roles you want to unmap.
5. In the *Roles* tab select the role that you want to remove, and click <.
6. Click *Update*.

   Members of the responsibility will no longer be able to access the BI platform, unless they have other accounts or aliases.

   > **i** 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.

5.9.3.4 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.

> **i** 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.

5.9.3.4.1 To schedule user updates

After you map roles into the BI platform, you need to specify how the system updates these roles.

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.

Recurrence pattern	Description
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.

> **i 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.

5.10 X.509 Authentication

5.10.1 X.509 Authentication for BI Launch Pad

5.10.1.1 Creating and Configuring Certificates and Keystores

> **i Note**
>
> A user should exist in the BI platform to achieve Single Sign-On through X.509 authentication.

> **i Note**
>
> Download and install OpenSSL toolkit to perform the steps below.

> **i 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 115] for creating and configuring certificates and keystores.

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.

5.10.1.1.1 With Trusted CA

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`

> ℹ 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.

5.10.1.2 Configuring Tomcat SSL Server

5.10.1.2.1 One-Way SSL Configuration

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.

5.10.1.2.2 Two-Way SSL Configuration

Configure the Tomcat server to request client authentication by following the steps below.

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*.

5.10.1.3 Configuring BI Launch Pad

5.10.1.3.1 Creating 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.

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\`

5.10.1.3.2 Passing the Shared Secret Key via the TrustedPrincipal.conf File

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'.

5.10.1.3.3 Editing the custom.jsp File

> **Note**
>
> Create a user with machine name in CMC before editing the custom.jsp file.

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 Creating a Shared Secret Key [page 118] to learn how to create a shared secret key.

5.10.1.3.4 Creating the myScript.js File

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.

5.10.1.3.5 Setting Up the BOE Internal and Custom Property Files

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.

5.10.1.3.6 Setting Up the BOE Web.xml Files

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.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.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.

5.10.2 X.509 Authentication for Web Services

5.10.2.1 For SOAP Web Services

5.10.2.1.1 Configuring SSL in Tomcat

When using web services, you need to configure SSL in Tomcat before configuring the SAP Business Intelligence platform.

i Note

A user should exist in the BI platform to achieve Single Sign-On through X.509 authentication.

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.

i Note

The password and location of the files mentioned above are just examples. You can add any password and location of your choice.

i Note

You can refer to Creating and Configuring Certificates and Keystores [page 113] for more information on creating and configuring keystore files.

5.10.2.1.2 Configuring the axis2.xml File

> **i 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`

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>
```

> **i 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.

5.10.2.1.3 Generating a Shared Secret Value

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.

> **i Note**
>
> You can view the shared secret value by opening TrustedPrincipal.conf in any XML editor.

5.10.2.1.4 Configuring web.xml File

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 Generating a Shared Secret Value [page 122].

```
<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.

> **i Note**
>
> The configurations made in the axis2.xml file will be discarded if you upgrade from a version lower than BI 4.2 SP04.

5.10.2.2 For RESTful Web Services

> **i 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. Refer Generating a Shared Secret Value in *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 the *Business Intelligence platform RESTful Web Service Developer Guide*.

5.10.3 X.509 Authentication for CMC

5.10.3.1 Editing the Custom.jsp File (For CMC)

> **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.

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.

5.10.3.2 Creating the myScript.js File (For CMC)

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.

5.10.3.3 Setting Up the BOE Internal and Custom Property Files (For CMC)

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.

5.10.3.4 Setting Up the BOE Web.xml File (For CMC)

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.servletbr
   idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
   ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
   bel.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`

> **i 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.

6 Managing User Attributes

6.1 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 Universe 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.

> **i** 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 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 64]
To import SAP roles [page 86]

6.3 To add a new user attribute

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.

> **i** 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.

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.

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.

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

6.4 To edit customized user attributes

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

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.

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

7 Multitenancy

7.1 Managing tenants in the CMC

After configuring tenants in the `tenant_template_def.properties` file and running the Multitenancy Management Tool to create tenants, you can manage the tenants in the Central Management Console (CMC).

To manage tenants, go to the *Multitenancy* management area of the CMC. You can perform the following tasks:

- Set some tenant properties, such as maximum concurrent users, and so on
- View user and group associations for a tenant
- Add a user group to or remove one from a tenant
- Delete a tenant

For more information about the `tenant_template_def.properties` file, see "Tenant definition configuration file reference".

1. To set tenant properties [page 130]
2. To assign access rights to a tenant user group [page 132]
3. To delete a tenant [page 134]

7.1.1 To set tenant properties

You can set the following properties, without modifying the tenant properties file, in the Central Management Console (CMC):

- Tenant name
- Description
- Keywords
- Concurrent users

You cannot edit these read-only tenant properties in the CMC:

- ID
- CUID
- Date created
- Date last modified

For detailed information about each property in the file, see "Tenant definition configuration file reference".

→ Tip

You can select a tenant and click on the toolbar to go directly to the *Properties* dialog box.

Parent topic: Managing tenants in the CMC [page 130]

Next task: To assign access rights to a tenant user group [page 132]

7.1.1.1 To change the name of the tenant

1. In the Central Management Console (CMC), select the *Multitenancy* area.
2. Double-click the tenant.
   The tenant *Properties* dialog box appears.
3. In the *Tenant Name* box, type a new name for the tenant.
4. Click *Save & Close*.
   The name you entered appears for the tenant.

7.1.1.2 To change the description of the tenant

1. In the Central Management Console (CMC), select the *Multitenancy* area.
2. Double-click the tenant.
   The tenant *Properties* dialog box appears.
3. In the *Description* box, type a description of the tenant.
4. Click *Save & Close*.
   The description you entered appears for the tenant.

7.1.1.3 To change keywords for the tenant

1. In the Central Management Console (CMC), select the *Multitenancy* area.
2. Double-click the tenant.
   The tenant *Properties* dialog box appears.
3. In the *Keywords* box, type keywords for the tenant
4. Click *Save & Close*.
   The keywords you entered appear for the tenant.

7.1.1.4 To change the number of concurrent users for a tenant

1. In the Central Management Console (CMC), select the *Multitenancy* area.
2. Double-click the tenant.
   The tenant *Properties* dialog box appears.
3. Under *Concurrent Users*, select the maximum number of concurrent users who can log on to the CMC for this tenant:
   - To enter a maximum number of users for this tenant who can log on to the CMC, select *Value*, and enter the number.
     If the maximum number is exceeded, a message appears and the user cannot log on.
   - If you do not want to limit the number of concurrent users for this tenant, select *Unlimited*.
4. Click *Save & Close*.
   The values you defined appear under the *Concurrent Users* column on the *Multitenancy* home page.

7.1.2 To assign access rights to a tenant user group

You can set access rights for tenant user groups in the Central Management Console (CMC), without modifying the properties file.

> → Tip
>
> You can select a tenant and click on the toolbar to go directly to the *User Security* dialog box.

1. In the CMC, select the *Multitenancy* area.
2. Right-click the tenant and select *User Security*.
3. In the *User Security* dialog box, click *Add Principals*.
4. In the *Add Principals* dialog box, move the tenant user group for which you want to set access rights from the *Available Users or Groups* list to the *Selected Users or Groups* list.
5. Click *Add and Assign Security*.
6. In the *Assign Security* dialog box, select access-right levels to grant to the tenant user group.
7. To enable folder inheritance, select the *Inherit From Parent Folder* check box.
   To disable group inheritance, clear the check box.
8. To enable group inheritance, select the *Inherit From Parent Group* check box.
   To disable group inheritance, clear the check box.
9. Click *OK*, and click *Close*.

The user group is assigned the access rights you selected.

Task overview: Managing tenants in the CMC [page 130]

Previous: To set tenant properties [page 130]

Next task: To delete a tenant [page 134]

7.1.2.1 To remove access rights from a tenant

You can remove access rights from a tenant user group in the Central Management Console (CMC), without modifying the properties file.

1. In the CMC, select the *Multitenancy* area.
2. Right-click the tenant and select *User Security*.
3. In the *User Security* dialog box, click *Add Principals*.
4. In the *Add Principals* dialog box, move the tenant user group for which to remove rights from the *Available Users or Groups* list to the *Selected Users or Groups* list.
5. Click *Add and Assign Security*.
6. In the *Assign Security* dialog box, click *Remove Access*.
7. Click *OK*, and click *Close*.

All access rights are removed from the tenant user group.

7.1.3 Managing user groups for a tenant

7.1.3.1 To view user and group associations for a tenant

You can view user and user group associations for a tenant in the Central Management Console (CMC), without modifying the properties file.

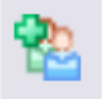
→ Tip

You can select a tenant and click on the toolbar to go directly to the *User Groups* dialog box.

1. In the CMC, select the *Multitenancy* area.
2. Double-click the tenant for which you want to view user and group associations.
3. In the *Properties* dialog box, click *User Groups* in the navigation list.
   The *User Groups* dialog box appears, listing the groups associated with this tenant.

7.1.3.2 To add a user group to a tenant

You can add a user group to a tenant in the Central Management Console (CMC), without modifying the properties file.

> → Tip
>
> You can select a tenant and click  on the toolbar to go directly to the *Add Groups to Tenant* dialog box.

1. In the CMC, select the *Multitenancy* area.
2. Right-click the tenant to add a user group to and select *Add Groups to Tenant*.
3. In the *Add Groups to Tenant* dialog box, move the user group to add from the *Available Groups* list to the *Selected Groups* list.
4. Click *OK*.

The user group is added to the tenant.

7.1.3.3 To remove a user group from a tenant

You can remove a user group from a tenant in the Central Management Console (CMC), without modifying the properties file.

1. In the CMC, select the *Multitenancy* area.
2. Double-click the tenant from which to remove a user group.
3. In the tenant *Properties* dialog box, click *User Groups* in the navigation list.
4. In the *User Groups* dialog box, select the user group to remove, and click *Remove*.

The user group is removed from the tenant.

7.1.4 To delete a tenant

You can delete tenants and all of their objects in the Central Management Console (CMC) from the BI repository.

> ℹ Note
>
> Objects that are shared, or where modification rights are not granted are not deleted.

> → Tip
>
> You can select a tenant and click on the toolbar to go directly to the *Delete* dialog box.

1. In the CMC, select the *Multitenancy* area.
2. Right-click a tenant, select *Delete*.
3. In the *Delete* dialog box, move the tenant to delete from the *Available* list to the *Excluded* list, and click *OK*.
4. In the confirmation dialog box that appears, click *OK* again.

The tenant is deleted from the Central Management Server (CMS) repository.

Task overview: Managing tenants in the CMC [page 130]

Previous task: To assign access rights to a tenant user group [page 132]

8 Managing License

8.1 Managing license keys

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

Related Information

To view license information [page 136]
To add a license key [page 136]
To view current account activity [page 137]

8.1.1 To view license information

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

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 136]
To view current account activity [page 137]

8.1.2 To add a license key

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.

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

The key is added to the list.

Related Information

To view license information [page 136]
To view current account activity [page 137]

8.1.3 To view current account activity

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 136]
To view license information [page 136]

9 Managing Servers

9.1 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. **i 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.

i 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.

9.2 To view a server's status

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.

   > **i** 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.

9.3 To start, stop, or restart servers with the CMC

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.

   > **i** 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*.

9.4 To automatically start a server

By default, servers in your deployment are automatically started when the Server Intelligence Agent starts. This task shows where to set the autostart option.

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*.

> **i 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.

9.5 To enable and disable servers with the CMC

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*.

9.6 Adding a server

You can run multiple instances of the same BI platform server on the same machine. To add a server:

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 >.

> **i 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.

9.7 To clone a server

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.

9.8 Deleting a server

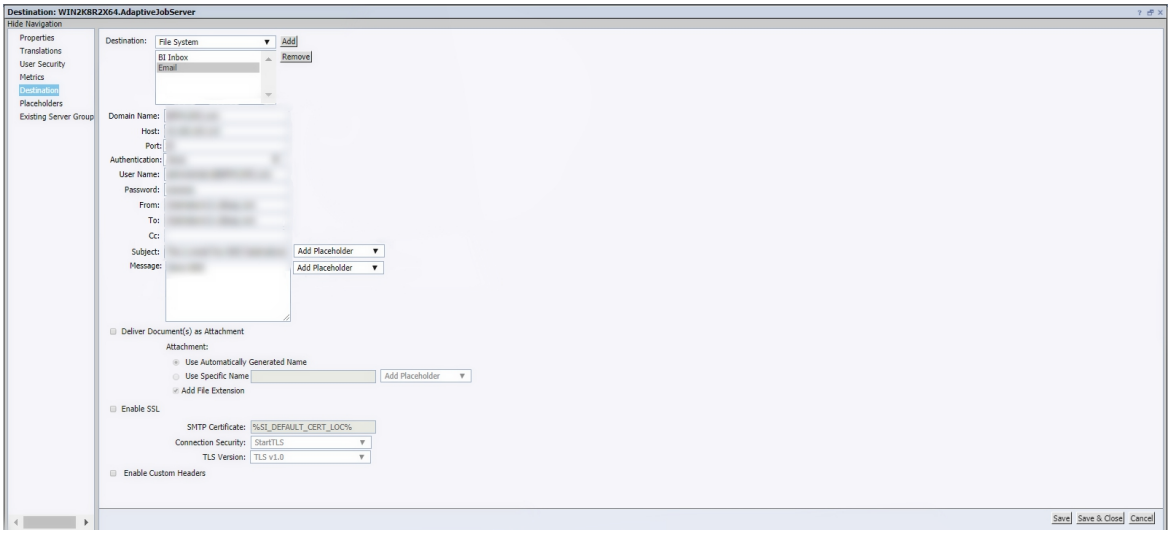
1. Go to the *Servers* management area of the CMC.
2. Stop the server that you want to delete.
3. Right-click the server and select *Delete*.
4. When prompted for confirmation, click *OK*.

9.9 Add Custom Internet Headers

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:

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*.

The emails with scheduled documents now contain the internet headers.

> **i 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.

9.10 To create a non-exclusive server group

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.

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.

   > i 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.

9.11 To add subgroups to a server group

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.

9.12 To make one server group a member of another

1. Go to the *Servers* management area of the CMC.
2. Click the group that you want to add to another group.

   > i 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*.

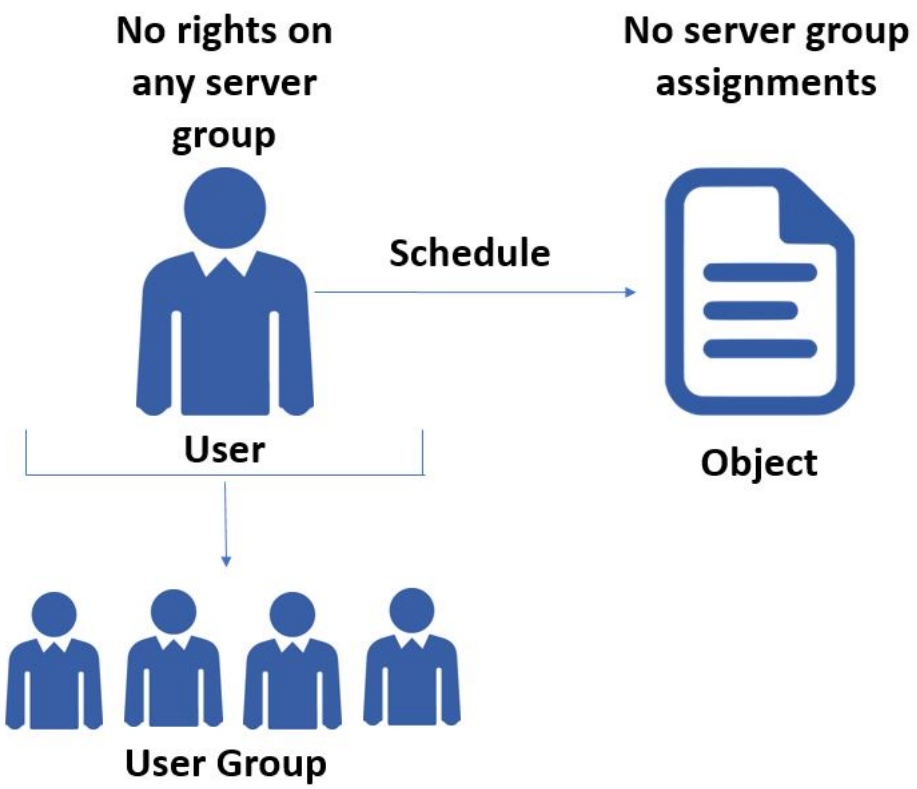
9.13 Understanding Server Group Rights Management

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.

> ℹ 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.

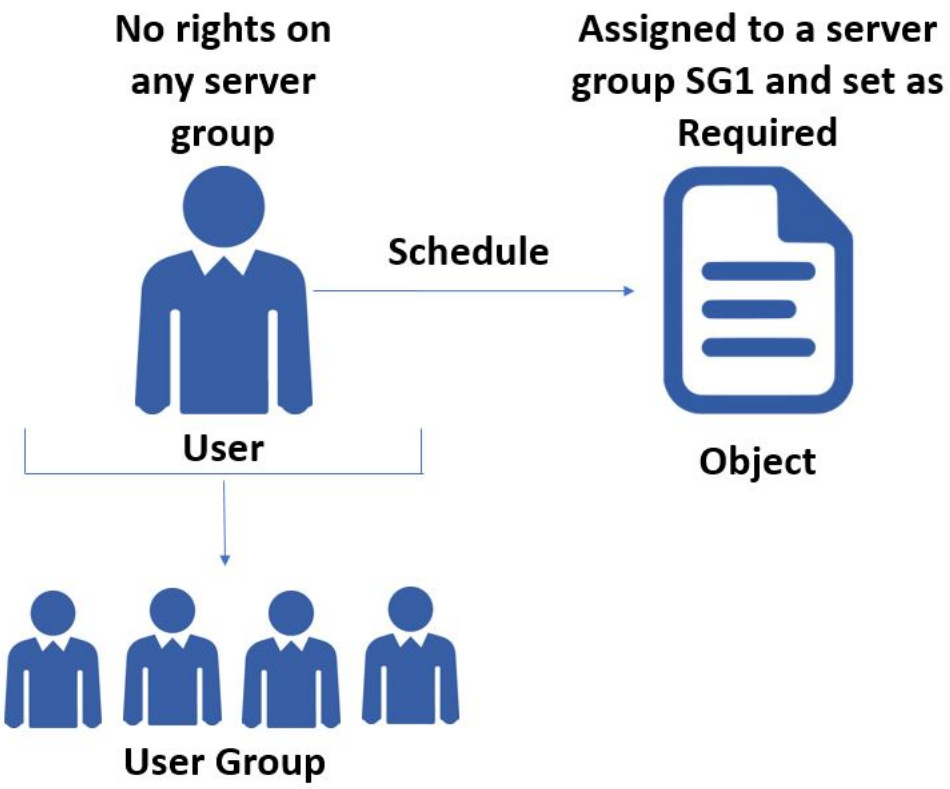
Scenario 1:

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.



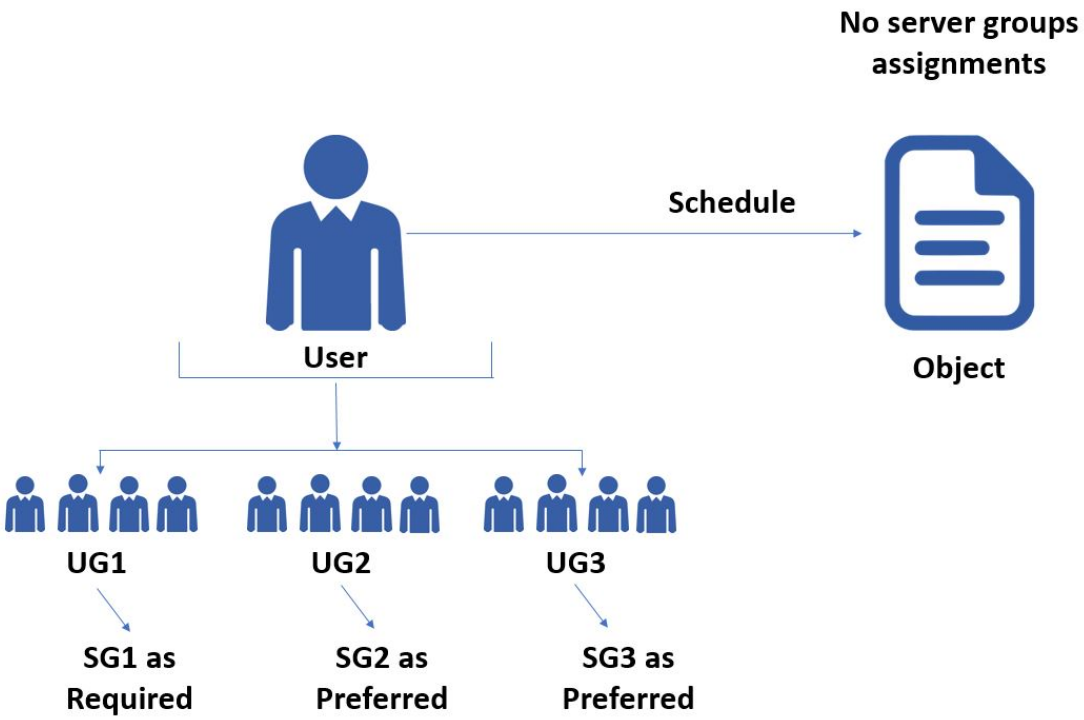
When a user schedules an object, the platform checks for server group assignments to the object. If a server group is assigned to the object, the platform checks whether the user has view rights on the server group.

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:

> **i** Note
>
> For scenarios 3 and 4, it is assumed that the user inherits the rights from its associated user groups.

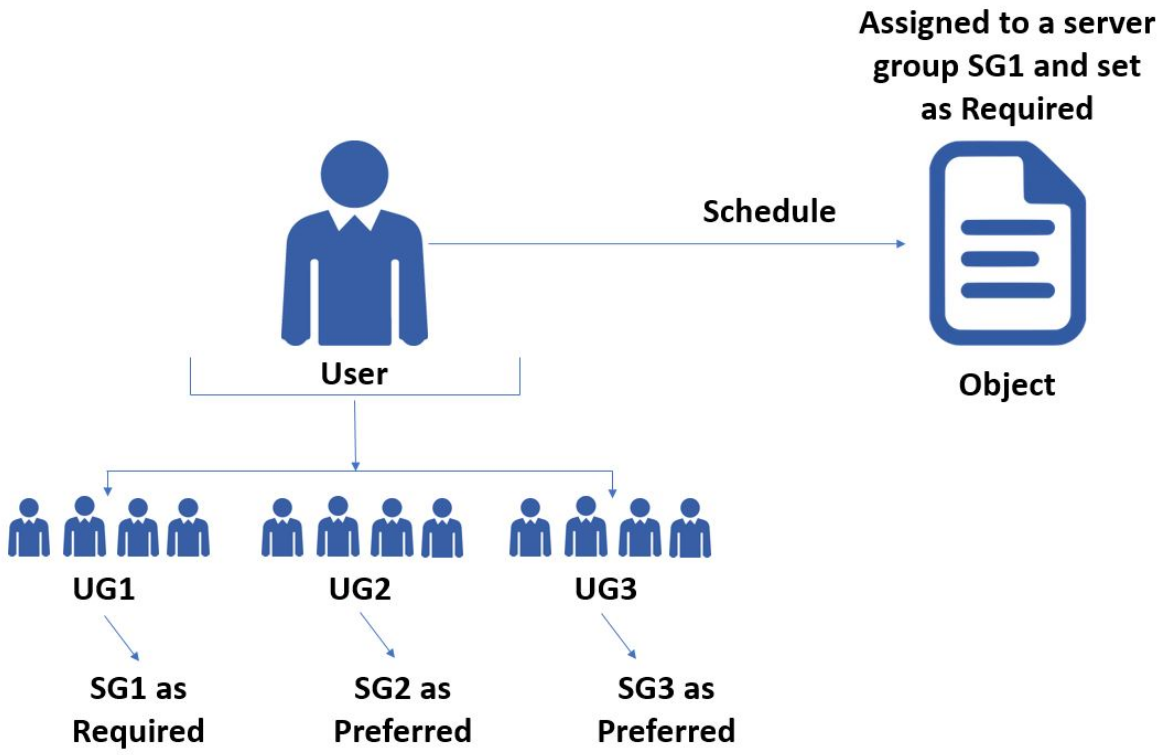
A user is a part of three user groups UG1, UG2, and UG3, and you have mapped each user group to server groups SG1, SG2, and SG3 respectively. SG1 is set as a Required server group however, and SG2 and SG3 are set as Preferred server groups. For more information on how to set a server group as Required 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:

ℹ 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

9.14 To modify a server's group membership

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.

   > **i 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*.

> **i 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.

9.15 To change a server's properties

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*.

> **i** 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.

9.16 To set a configuration template

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.

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*.

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.

> **i** 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 153]

9.17 To apply a configuration template to a server

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.

> **i** 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.

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*.

   > **i** 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.

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 152]

9.18 To restore system defaults

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).

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.

9.19 To view server metrics

1. Go to the *Servers* management area of the CMC.
2. Right-click the server whose metrics you want to view, and select *Metrics*.

The *Metrics* tab displays a list of metrics for the server.

Related Information

To change a server's properties [page 152]
About the Server Metrics Appendix [page 475]

9.20 To view system metrics

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.

9.21 To enable or disable destinations for a job server

For an Adaptive Job Server to store output instances in a destination other than the default, you have to enable and configure the other destinations on the job servers.

> **i** Note
>
> The managed (Inbox) destination is enabled and configured by default on all job servers. This allows you to use the "Send to" feature and to distribute reports to users within the BI platform system. If you want, you can enable and configure additional destinations on the server.

1. Go to the *Servers* management area of the CMC.
2. Select the job server for which you want to enable or disable a destination.
3. Choose *Properties* from the *Manage* menu.
4. In the *Properties* dialog box, click *Destinations* in the navigation list
5. To enable a destination, select it in the *Destination* list and click *Add*.
6. To disable a destination, select it in the *Destination* list and click *Remove*.
7. Click *Save* or *Save & Close* .

Related Information

To set the destination properties for a job server [page 156]

9.22 To view server placeholders

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 493]

9.23 To view and edit the placeholders for a node

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.

> ℹ 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 493]

9.24 To set the destination properties for a job server

1. Go to the *Servers* management area of the CMC.
2. Select the job server whose setting you want to change.
3. Choose *Properties* from the *Manage* menu.
4. In the *Properties* dialog box, click *Destinations* in the navigation list
5. Select a destination from the list, then click *Add*.
6. Set the properties for the destination.
7. Click *Save* or *Save & Close*.
8. Make sure the destination has been enabled.

Related Information

To enable or disable destinations for a job server [page 154]
Inbox destination properties [page 156]
File System destination properties [page 160]
FTP destination properties [page 158]
Email destination properties [page 157]

9.24.1 Inbox destination properties

The Inbox destination stores an object or instance in the user inboxes on the BI platform system. A user inbox is automatically created when you add a user.

> **i** Note
>
> On the Destination Job Server, the managed (Inbox) destination is enabled and configured by default on all job servers. This allows you to use the "Send to" feature and to distribute reports to users within the BI platform system. If you want, you can enable and configure additional destinations on the Adaptive Job Server.

Send list

Specify which users or user groups you want to receive instances from that have been generated or processed by the job server.

Target Name

Use the default automatically-generated name for the instance, or provide a specific name. You can add variables to the specific name by clicking them in the *Add placeholder* list.

Send document as

Select the options you want:

- *Shortcut*
  The system sends a shortcut to the specified destination.
- *Copy*
  The system sends a copy of the object instance to the destination.

9.24.2 Email destination properties

The following settings are available for email destinations.

Domain Name

Enter the fully qualified domain of the SMTP server.

Host

Enter the name of the SMTP server.

Port

Enter the port that the SMTP server is listening on. (This standard SMTP port is 25.)

Authentication

Select Plain or Login if the job server must be authenticated using one of these methods in order to send email.

User Name

Provide the Job Server with a user name that has permission to send email and attachments through the SMTP server.

Password

Provide the Job Server with the password for the SMTP server.

From

Provide the return email address. Users can override this default when they schedule an object.

To, Cc, Subject, and Message

Set the default values for users who schedule reports to this SMTP destination. Users can override these defaults when they schedule an object.

Add placeholder

You can add placeholder variables to the message body using the *Add placeholder* list. For example, you can add the report title, author, or the URL for the viewer in which you want the email recipient to view the report.

Add Attachment

Select this check box if you want to attach a copy of the report or program instance to the email. When you add an attachment, you can choose between the following naming conventions:

- *Automatically Generated*
  Select this option if you want the BI platform to generate a random file name.
- *Specific Name*
  Select this option if you want to enter a file name. You can also add a variable to the file name. To add a variable, choose a placeholder for a variable property from the *Add placeholder* list.

- *Add File Extension*
  Adds the .%EXT% extension to the specified filename. This is similar to selecting File Extension from the *Add placeholder* list. By adding an extension to the file name, Windows will know which program to use to open the file.

> **Note**
>
> Users can override these settings when they schedule an object.

9.24.2.1 Setting up SMTP over SSL

To setup SMTP over SSL, it is required that the same certificate be present in the Server and the Client systems.

To setup SMTP over SSL, follow the below mentioned steps:

1. On the Windows platform, go to `<install_dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.In addition for clients connected to the BI Platform, go to `<install_dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.`

   > **Note**
   >
   > For all other supported platforms, navigate to the respective folders.

2. Name the certificate as "certificate.crt".

   For example, While connecting to the SMTP server, the server will send the certificate detail. The certificate detail needs to copied to a raw text file and renamed as “certificate.crt”. This must be placed in the win64_x64 folder for the windows platform and in the win32_86 folder for the clients.

SMTP over SSL is now setup.

> **Note**
>
> When the user checks the *Enable SSL* checkbox, a secure channel is enabled. This allows secure SMTP transmission over SSL.

9.24.3 FTP destination properties

The following settings are available for FTP destinations.

Host

Enter your FTP host information.

Port

Enter the FTP port number (the standard FTP port is 21).

User Name

Specify a user who has the necessary rights to upload a report to the FTP server.

Password

Enter the user's password.

Account

Enter the FTP account information, if required.

Account is part of the standard FTP protocol, but it is rarely implemented. Provide the appropriate account only if your FTP server requires it.

Directory

Enter the FTP directory that you want the object to be saved to. A relative path is interpreted relative to the root directory on the FTP server.

Automatically Generated

Select this option if you want the BI platform to generate a random file name.

Specific Name

Select this option if you want to enter a file name—you can also add a variable to the file name. To add a variable, choose a placeholder for a variable property from the list.

Add File Extension

Adds the .%EXT% extension to the specified filename. This is similar to selecting File Extension from the *Add placeholder* list. By adding an extension to the file name, Windows will know which program to use to open the file.

9.24.4 SFTP destination properties

The following settings are available for SFTP destinations.

Host

Enter your SFTP host information.

Port

Enter the SFTP port number (the standard SFTP port is 22).

User Name

Specify a user who has the necessary rights to upload a report to the SFTP server.

Password

Enter the user's password.

Account

Enter the SFTP account information, if required.

Account is part of the standard SFTP protocol, but it is rarely implemented. Provide the appropriate account only if your SFTP server requires it.

Directory

Enter the SFTP directory that you want the object to be saved to. A relative path is interpreted relative to the root directory on the SFTP server.

Automatically Generated

Select this option if you want the BI platform to generate a random file name.

Specific Name

Select this option if you want to enter a file name—you can also add a variable to the file name. To add a variable, choose a placeholder for a variable property from the list.

Fingerprint

Enter the host key fingerprint of the SFTP server.

Add File Extension

Adds the .%EXT% extension to the specified filename. This is similar to selecting File Extension from the *Add placeholder* list. By adding an extension to the file name, Windows will know which program to use to open the file.

9.24.5 File System destination properties

A file system destination is an unmanaged disk destination on a system outside the BI platform system.

Directory

Type the absolute path to the directory. The directory can be on a local drive of the Adaptive Job Server machine, or on any other machine that you can specify with a UNC path.

Automatically Generated

Select this option if you want BI platform to generate a random file name.

Specific Name

Select this option if you want to enter a file name—you can also add a variable to the file name. To add a variable, choose a placeholder for a variable property from the list.

Add File Extension

Adds the .%EXT% extension to the specified filename. This is similar to selecting File Extension from the *Add placeholder* list. By adding an extension to the file name, Windows will know which program to use to open the file.

User Name

Specify a user who has permission to write files to the destination directory.

Password

Type the password for the user.

In this example, the destination directory is on a network drive that is accessible to the Adaptive Job Server machine through a UNC path. Each file name will be randomly generated, and a user name and password have been specified to grant the Adaptive Job Server permission to write files to the remote directory.

9.25 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.
  The wizard is available from the Central Management Console (CMC). For more information about the wizard, see Introduction to the System Configuration Wizard [page 18]. For more information about default deployment templates, see the *SAP BusinessObjects BI platform Deployment Templates* document, which is available from within the wizard, and also at http://help.sap.com/bobip41.
- Use the CMC to manually create and configure additional APSs. For details, see Adding a server [page 142].

> → Remember
>
> Selecting a deployment template in the wizard or manually creating additional APSs does not replace system sizing. Ensure that sizing is performed: http://www.sap.com/bisizing.

10 Managing Web Application Container Servers (WACS)

10.1 Web Application Container Server (WACS)

Web Application Container Servers (WACS) provide a platform for hosting SAP BusinessObjects Business Intelligence platform web applications. For example, a Central Management Console (CMC) can be hosted on a WACS.

WACS simplifies system administration by removing several workflows that were previously required for configuring application servers and deploying web applications, and by providing a simplified, consistent administrative interface.

Web applications are automatically deployed to WACS. WACS does not support manual or WDeploy deployment of BI platform or external web applications.

10.2 Adding or removing additional WACS to your deployment

Adding additional WACS to your deployment can give you a number of advantages:

- Faster recovery from a misconfigured server.
- Improved server availability.
- Better load balancing.
- Better overall performance.

There are three ways to add additional WACS to your deployment:

- Installing WACS on a machine.
- Creating a new WACS.
- Cloning a WACS.

> **i** Note
>
> It is recommended that you run a single WACS on the same machine at the same time due to high resource utilization. However, you can deploy more than one WACS on the same machine, and only run one of them, to help you recover in the event of a misconfigured WACS.

10.2.1 Installing WACS

Installing WACS on separate machines can provide your deployment with better performance, better load balancing, and higher server availability. If your deployment contains two or more WACS on separate machines, the availability of web applications and web services won't be affected by hardware or software failures on a specific machine, because the other WACS will continue to provide the services.

You can install a Web Application Container Server by using the BI platform installation program. There are two ways that you can install WACS:

- In a Full installation, on the *Select Java Web Application Server* screen, choose *Install the Web Application Container Server and automatically deploy web applications*.
  If you select a Java application server in a New installation, WACS is not installed.
- In a Custom / Expand installation, you can choose to install WACS on the *Select Features* screen by expanding *Servers* > *Platform Services* and selecting *Web Application Container Server*.

If you install WACS, the installation program automatically creates a server called `<NODE>.WebApplicationContainerServer`, where `<NODE>` is the name of your node. BI platform web applications and web services are then deployed to that server. No manual steps are required to deploy or configure the CMC. The system is ready to use.

When you install WACS, the installation program prompts you to provide an HTTP port number for WACS. Ensure that you specify a port number that is not used. The default port number is 6405. If you plan to allow users to connect to the WACS from outside a firewall, you must ensure that the server's HTTP port is open on the firewall.

> **Note**
>
> The web applications that WACS hosts are automatically deployed when you install WACS or when you apply updates or hot-fixes to WACS or to WACS-hosted web applications. It takes several minutes for the web applications to deploy. The WACS will be in the "Initializing" state until the web application deployment is complete. Users will not be able to access web applications hosted on WACS until the web applications are fully deployed. Do not stop the server until the initial deployment is completed. You can view the server state of the WACS through the Central Configuration Manager (CCM).
>
> This delay occurs only when starting WACS the first time after installing WACS or applying updates to it. This delay does not occur for subsequent WACS restarts.
>
> Web applications cannot be manually deployed to a WACS server. You cannot use WDeploy to deploy web applications to WACS.

10.2.2 Adding a new Web Application Container Server

> **Note**
>
> It is recommended that you run a single WACS on the same machine at the same time due to high resource utilization. However, you can deploy more than one WACS on the same machine, and only run one of them, to help you recover in the event of a misconfigured WACS.

1. Go to the *Servers* management area of the CMC.
2. Select *Manage* > *New* > *New Server*.
   The *Create New Server* screen appears.
3. From the *Service Category* list, select *Core Services*.
4. From the *Select Service* list, select the services that you want the WACS to host, and click *Next*.
   - If you want the WACS to host web applications such as the CMC, BI launch pad or OpenDocument, select *BOE Web Application Service*.
   - If you want the WACS to host web services such as Live Office or Query as a Web Service (QaaWS), select *Web Services SDK and QaaWS Service*.
   - If you want the WACS to host Business Process BI Web Services, select *Business Process BI Web Service*.
5. On the next *Create New Server* screen, select any additional services that you want the WACS to host, and click *Next*.
6. On the next *Create Server Screen*, select a node to add the server to, type a server name and description for the server, and click *Create*.

   > **Note**
   >
   > Only those nodes that have WACS installed will appear in the *Node* list.

7. On the *Servers* screen, double-click the new WACS.
   The *Properties* screen appears.
8. If you do not want the WACS to automatically start when the system restarts, in the *Common Settings* pane, ensure that the *Automatically start this server when the Server Intelligence Agent starts* check box is unchecked.
9. Click *Save & Close.*

A new WACS is created. The default settings and properties are applied to the server.

10.2.3 Cloning a Web Application Container Server

As an alternative to adding a new WACS to your deployment, you can also clone a WACS, either to the same machine or to another machine. While adding a new WACS creates a server with the default settings, cloning a WACS applies the settings of the source WACS to the new WACS.

Servers can only be cloned to machines that already have WACS installed.

> **Note**
>
> It is recommended that you run a single WACS on the same machine at the same time due to high resource utilization. However, you can deploy more than one WACS on the same machine, and only run one of them, to help you recover in the event of a misconfigured WACS.

1. Go to the *Servers* management area of the CMC.
2. Select the WACS that you want to clone, right-click and select *Clone Server*.

   The *Clone Server* screen displays a list of nodes in your deployment that you can clone the WACS to. Only those nodes that have WACS installed appear in the *Clone to Node* list.

3. On the *Clone Server* screen, type a new server name, select the node that you want to clone the server to, and click *OK*.

A new WACS is created. The new server contains the same services as the server that it is cloned from. The new server and services that it hosts have the same settings as the server it was cloned from, with the exception of the server name.

> **i** Note
>
> If you cloned a WACS to the same machine, you may have port conflicts with the WACS that was used for cloning. If this occurs, you must change the port numbers on the newly cloned WACS instance.

Related Information

To resolve HTTP port conflicts [page 172]

10.2.4 Deleting WACS from your deployment

You can only delete a WACS if the server isn't currently serving the CMC to you. If you want to delete a WACS from your deployment, you must log on to a CMC from another WACS or a Java application server. You cannot delete a WACS that is currently serving the CMC to you.

1. Go to the *Servers* management area of the CMC.
2. Stop the server that you want to delete by right-clicking the server and clicking *Stop Server*.
3. Right-click the server and select *Delete*.
4. When prompted for confirmation, click *OK*.

10.3 Adding or removing services to WACS

10.3.1 To add a web application or web service to a WACS

Adding additional BI platform web applications or web services to a WACS requires that you stop the WACS. Therefore, you must have at least one additional CMC hosted on a WACS in your deployment that provides a BOE Web Application Service while you are stopping and adding a service to the other WACS.

When you add a service to WACS, the service is automatically deployed to WACS when the server is restarted.

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to add the service to, and view the properties of the server to ensure that the service that you want to add is not already present.
3. Click *Cancel* to return to the *Servers* screen.

4. Stop the server by right-clicking the server and clicking *Stop Server*.

   If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running BOE Web Application Service on another WACS in your deployment. If you do, click *OK*, log on to another WACS, and start this procedure from the beginning.
5. Right-click the server and choose *Select Services*.
   The *Select Services* screen appears.
6. Select the service that you want to add to the server, add the service to the server by clicking >, and click *OK*.
7. Start the WACS by right-clicking the server and clicking *Start Server*.

The service is added to the WACS. The default settings and properties for the service are applied.

10.3.2 To remove a web application or web service from a WACS

In order to remove a web application or web service from a WACS, you must log on to a CMC on another WACS or on a Java application server. You cannot stop the WACS that is currently serving the CMC to you.

You cannot delete the last service from a WACS. Therefore, if you are removing a web service from a WACS, you must ensure that the server is hosting at least one other service.

If you want to remove the last service from a WACS, delete the WACS itself.

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to remove the web service from, and view the properties of the server to ensure that the web service that you want to remove is present.
3. Click *Cancel* to return to the *Servers* screen.
4. Stop the WACS by right-clicking the server and clicking *Stop Server*.

   If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running BOE Web Application Service on another WACS in your deployment. If you do, click *OK*, log on to another WACS, and start this procedure from the beginning.
5. Right-click the WACS and choose *Select Services.*
   The *Select Services* screen appears.
6. Select the service that you want to remove, click <, and then click *OK*.
7. Start the WACS by right-clicking the server and clicking *Start Server*.

The service is removed from the WACS.

10.4 To configure WACS for AD Kerberos

To configure AD Kerberos authentication for WACS, you must first configure your machine to support AD. You must perform the following steps.

- Enabling the Windows AD security plug-in.
- Mapping users and groups.
- Setting up a service account.
- Setting up constrained delegation.
- Enabling Kerberos authentication in the Windows AD plug-in for WACS.
- Creating configuration files.

For more information on performing these tasks, see the "Managing Web Application Container Servers (WACS)" chapter of the *BI platform Administrator Guide*.

After you've setup the machine that is hosting WACS to use AD Kerberos authentication, you must perform these steps through the Central Management Console (CMC).

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to configure AD for.
   The *Properties* screen appears.
3. In the *Krb5.ini File Location* field, specify the path to the `krb5.ini` configuration file.
4. In the *bscLogin.conf File Location* field, specify the path to the `bscLogin.conf` configuration file.
5. Click *Save & Close*.
6. Restart the WACS.

10.5 To configure WACS AD Kerberos single sign-on

If you are configuring AD Kerberos single sign-on for BI launch pad or Web Services SDK and QaaWS hosted on WACS, you must ensure that you have configured the machine that is hosting WACS for AD Kerberos authentication and AD Kerberos single sign-on. For more information, see the "Managing Web Application Container Servers (WACS)" chapter of the *BI platform Administrator Guide*.

After you've setup the machine that is hosting WACS to use AD Kerberos authentication and single sign-on, you must perform these steps through the Central Management Console (CMC).

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to configure.
   The *Properties* screen appears.
3. Check *Enable Kerberos Active Directory Single Sign On*.
4. Specify values for Default AD Domain, Service Principal Name, and Keytab File properties, and click *Save & Close* .
5. Restart the WACS.

10.6 To configure HTTPS/SSL

Before you configure HTTPS/SSL on your WACS, ensure that you've already created a PCKS12 file or JKS keystore, and that you've copied or moved the file to the machine that is hosting the WACS.

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS the server for which you want to enable HTTPS.
   The *Properties* screen appears.
3. In the *HTTPS Configuration* section, check the *Enable HTTPS* check box.
4. In the *Bind to Hostname or IP Address* field, specify the IP address for which the certificates were issued and to which WACS will bind.
   HTTPS services will be provided through an IP address that you specify.
5. In the *HTTPS Port* field, specify a port number for WACS to provide HTTPS service. You must ensure that this port is free. If you plan to allow users to connect to the WACS from outside a firewall, you must also ensure that this port is open on the firewall.
6. If you are configuring SSL with a reverse proxy, specify the proxy server's hostname and port in the *Proxy Hostname* and *Proxy Port* fields.
7. On the *Protocol* list, select a protocol. The available options are:
   - *SSL*
     SSL is the Secure Sockets Layer protocol, which is a protocol for encrypting network traffic.
   - *TLS*
     TLS is the Transport Layer Security protocol, and is a newer, enhanced protocol. The differences between SSL and TLS are minor, but include stronger encryption algorithms in TLS.
8. Under the *Certificate Store Type* field, specify the file type for the certificate. The available options are:
   - *PKCS12*
     Select PKCS12 if you are more comfortable working with Microsoft tools.
   - *JKS*
     Select JKS if you are more comfortable working with Java tools.
9. In the *Certificate Store File Location* field, specify the path where you copied or moved the certificate file store or Java keystore file.
10. In the *Private Key Access Password* field, specify the password.

    PKCS12 certificate stores and JKS keystores have private keys that are password protected, to prevent unauthorized access. You must specify the password for accessing the private keys, so that WACS can access the private keys.
11. It is recommended that you either use a certificate file store or keystore that either contains a single certificate, or where the certificate that you want to use is listed first. However, if you are using a certificate file store or keystore that contains more than one certificate, and that certificate is not the first one in the filestore, in the *Certificate Alias* field, you must specify the alias for the certificate.
12. If you want the WACS to only accept HTTPS requests from certain clients, enable client authentication.

    Client authentication doesn't authenticate users. It ensures that WACS only serves HTTPS requests to certain clients.
    a. Check *Enable Client Authentication*.
    b. In the *Certificate Trust List File Location*, specify the location of the PCKS12 file or JKS keystore that contains the trust list file.

> **i Note**
>
> The Certificate Trust List type must be the same as the Certificate Store type.

> **Note**
>
> Refer For RESTful Web Services [page 123] for more information on establishing trusted authentication using X.509 certificates.

> **Note**
>
> You can import an ABAP system's certificate into the BI Platform by executing the command: `keytool -import -trustcacerts -alias <Alias_Name> -file <CA_certificate_path> -keystore <trust_keystore_path>` . Refer the table below to understand the command:

Command	Description
-alias	Alias Name
-file	File path of the ABAP system's certificate
-keystore	File path of the Trusted keystore

c. In the *Certificate Trust List Private Key Access Password* field, type the password that protects the access to the private keys in the Certificate Trust List file.

> **Note**
>
> If you enable client authentication, and a browser or web service consumer is not authenticated, the HTTPS connection is rejected.

13. Click *Save & Close*.
14. Go to the *Metrics* screen, and ensure that HTTPS connector appears under *List of Running WACS Connectors*. If HTTPS does not appear, then ensure that the HTTPS connector is configured correctly.

10.7 WACS and your IT environment

This section describes how to configure WACS in a complex environment.

10.7.1 Using WACS with a reverse proxy

You can use WACS in a deployment with a forward or reverse proxy server. You cannot use WACS itself as a proxy server.

10.7.1.1 To configure WACS to support HTTP with a reverse proxy

To use WACS in a deployment with a reverse proxy, configure your WACS so that the HTTP Port is used for communication inside a firewall (for example on a secure network), and the HTTP through Proxy port is used for communication from outside the firewall (for example, the Internet).

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to configure.
   The *Properties* screen appears.
3. In the *Configuration of HTTP through Proxy* section:
   a. Check *Enable HTTP through Proxy*.
   b. Specify the HTTP port of the WACS to be used for communication through the proxy.
   c. Specify the Proxy Hostname and Proxy Port of the proxy server.
4. Click *Save & Close*.

10.7.1.2 To configure WACS to support HTTPS with a reverse proxy

Some load balancers and reverse proxy servers can be configured to decrypt HTTPS traffic and then forward the decrypted traffic to your application servers. In this case, you can configure WACS to use HTTP or HTTP through proxy.

If your load balancer or reverse proxy forwards HTTPS traffic, and you want to configure HTTPS with a reverse proxy, create two WACS. Configure one WACS for HTTPS for external traffic through the reverse proxy, and the other WACS to communicate with clients on your internal network through HTTPS.

10.7.2 To configure WACS on a multihomed machine

A multihomed machine is one that has multiple network addresses. By default, a Web Application Container Server instances binds its HTTP port to all IP addresses. If you want to bind WACS to a specific Network Interface Card (NIC), for example, when you want to bind the HTTP port of the WACS to one NIC and bind the request port to another NIC:

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to configure.
   The *Properties* screen appears.
3. In the *Configuration of HTTP through Proxy* section of the *Web Application Container Service* pane, uncheck *Bind to All IP Addresses*, and type an IP address for the WACS to bind to.
4. In the *HTTP Configuration* section, uncheck *Bind to All IP Addresses*, and type an IP address or hostname for the WACS to bind to.
5. Under *Common Settings*, deselect *Auto assign*, and then specify the Hostname or IP Address of the NIC that's used for communication between WACS and the other BI platform servers in your deployment.

6. Click *Save & Close*.
7. Restart the WACS.

10.8 Troubleshooting

10.8.1 To view server metrics

You can view the server metrics of a WACS from the Central Management Console (CMC).

1. Go to the *Servers* management area of the CMC.
2. Right-click the WACS, and click *Metrics*.

Related Information

Web Application Container Server Metrics [page 486]

10.8.2 To view the state of a WACS

To view the state of a WACS, go to the *Servers* area of the CMC. The *Servers List* includes a *State* column that provides the state for each server in the list.

WACS has a server state called "Running with Errors". This state means that the WACS is running, but has one or more of these error conditions:

- An HTTP, HTTP through Proxy, or HTTPS connector is misconfigured.
- A service running on WACS, such as the Tracelog service, is not running properly.
- A web application has failed to deploy in WACS.

See the WACS *Properties* page to see which services have failed.

10.8.3 Resolving port conflicts

If you cannot get any pages when you try to access the CMC through a particular port, ensure that another application has not taken over the HTTP, HTTP through proxy, or HTTPS ports that you have specified for WACS.

There are two ways to determine if there are port conflicts with your WACS. If you have more than one WACS in your deployment, log on to the CMC and check the List of Running WACS Connectors and WACS Connector(s) Failed at Startup metrics. If the HTTP, HTTP through Proxy, or HTTP connectors do not appear in the List of Running WACS Connectors, these connectors are not able to start due to a port conflict.

If your deployment has only one WACS, or If you are not able to access the CMC through any WACS, use a utility such as netstat to determine if another application has taken a WACS port.

10.8.3.1 To resolve HTTP port conflicts

1. Start the Central Configuration Manager (CCM), and click the *Manage Servers* icon.
2. Specify the logon credentials.
3. On the *Manage Servers* screen, stop the WACS.
4. Click the *Web Tier Configuration* icon.

   > **i** Note
   >
   > The *Web Tier Configuration* icon is only enabled when you select a WACS that is stopped.

   The *Web Tier Configuration* screen appears.
5. In the *HTTP Port* field, specify a free HTTP port to be used by the Web Application Container Server, and click *OK*.
6. On the *Manage Servers* screen, start the WACS.

10.8.3.2 To resolve HTTP through proxy or HTTPS port conflicts

If you cannot access a WACS through the HTTP through proxy or HTTPS ports, but you can still connect to the Central Management Console (CMC) through the HTTP port, change the port numbers through the CMC.

1. Go to the *Servers* management area of the CMC.
2. To stop the WACS that you want to configure, right-click the server and click *Stop Server*.
3. Double-click the WACS that you want to configure.
   The *Properties* screen appears.
4. In the *Configuration of HTTP through Proxy* section, specify a new HTTP port.
5. To change the HTTPS port, in the *HTTPS Configuration* section, type a new value in the *HTTPS Port* field.
6. Click *Save & Close*.
7. To start the WACS, right-click the server and click *Start Server*.

10.8.4 To change the number of concurrent requests

The default number of concurrent HTTP requests that WACS is configured to handle is 150. This should be acceptable for most deployment scenarios. To improve the performance of WACS, you can increase the maximum number of concurrent HTTP requests. Although increasing the number of concurrent requests can improve performance, setting this value too high can hurt performance. The ideal setting depends on your hardware, software, and IT requirements.

1. Go to the *Servers* management area of the CMC.
2. To stop the WACS that you want to configure, right-click the server and click *Stop Server*.
3. Double-click the WACS that you want to configure.
   The *Properties* screen appears.
4. Under *Concurrency Settings (Per Connector)*, in the *Maximum Concurrent Requests* field, type the desired number of concurrent requests, and click *Save & Close*.
5. To start the WACS, right-click the server and click *Start Server*.

10.8.5 To prevent users from connecting to WACS through HTTP

In certain cases, you may want to allow only users from the local machine to connect to a WACS through HTTP or HTTPS. For example, although you cannot close the HTTP port, you may want to configure your WACS so that it accepts only HTTP requests from the clients located on the same machine as the WACS. In this way, you can perform maintenance or configuration tasks on the WACS through a browser from the same machine as the WACS, while preventing other users from accessing the server.

1. Go to the *Servers* management area of the CMC.
2. Double-click the WACS that you want to modify.
   The *Properties* screen appears.
3. In the *Web Application Container Service* section, clear the *Bind to All IP Addresses* check box.
4. In the *Bind to Hostname or IP Address* field, type **`127.0.0.1`**, and click *Save & Close*.
5. To start the WACS, right-click the server and click *Start Server*.
   The WACS that is configured this way accepts only connections from the local machine.

11 Managing Applications

11.1 Overview

The *Applications* management area of the CMC allows you to change the appearance and functionality of web applications such as the CMC and Fiorified 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 edition for OLAP*
- *Analysis Office Runtime*
- *BEx Web Applications*
- *BI Administrators' Cockpit*
- *Fiorified BI launch pad*
- *BI workspaces*
- *Central Management Console*
- *Collaboration*
- *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*
- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*
- *Translation management tool*
- *Universe design tool*
- *Version Management*
- *Version Management*
- *Visual Difference*
- *Web Intelligence*

- *Web Service*
- *Workflow Assistant*

11.2 General settings

11.2.1 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*.

11.2.2 To set the web application trace log level in the CMC

To trace other web applications, you must manually configure the corresponding `BO_trace.ini` file.

1. In the *Applications* area of the CMC, right-click an application and select *Trace Log Settings*.

   > **i 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.

The new trace log level will take effect after the next web application logon.

Related Information

Trace log levels [page 175]

11.2.2.1 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.

11.3 Application settings

11.3.1 Managing CMC tab access

11.3.1.1 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 178]
To manage permission to configure CMC tab access for other users or user groups [page 180]

11.3.1.2 Working with CMC tab access

11.3.1.2.1 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).

11.3.1.2.1.1 To manage CMC tab access for other users

1. Log on to the CMC.
2. On the *Users and Groups* tab, right-click a principal and select *CMC Tab Configuration*.

   > ℹ 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.

   > ℹ Note
   >
   > Clicking the buttons applies changes to the principal immediately.

4. When you are finished, click *Close*.

The new effective tab access is displayed in the *Permission* column of the table.

Related Information

To restrict CMC tab access [page 181]

11.3.1.2.1.2 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.

> **i** 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.

11.3.1.2.1.3 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.

> **i** 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*,

Delegated Administrator User Group	Recommended Rights
	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*.

11.3.1.2.1.4 To manage permission to configure CMC tab access for other users or user groups

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.

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.

   > **i 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.

   > **i Note**
   >
   > Selecting a setting from the list changes the permission of the principal immediately.
4. When you are finished, click *Close*.

The new effective permission is displayed.

Related Information

Delegated administration and CMC tab access [page 176]
Inheritance of CMC tab access [page 179]

11.3.1.2.1.5 To add a Customization tab for a user or user group

CMC tab access must be set to "Restricted" before you can add a *Customization* tab for a user or user group.

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*.

11.3.1.2.2 To restrict CMC tab access

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.

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).

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*.

The CMC tab access rule is applied to the system.

Related Information

To troubleshoot CMC tab access [page 182]

11.3.1.2.3 To troubleshoot CMC tab access

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.

1. Log onto the CMC as an administrator.

   > **i 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.

   > **i 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 178]
Inheritance of CMC tab access [page 179]

11.3.2 Managing BI launch pad settings

In the *Applications* area of the CMC in the BI platform, select *Manage* > *Properties* to view display options for BI launch pad.

For BI launch pad, you can grant users or groups the following abilities:

- Changing preferences
- Organizing folders
- Searching
- Filtering object listings by object type
- Viewing the `Favorites` folder

For example, if you created user folders using a standard naming convention, you can deny users the ability to organize their own folders.

> **Note**
>
> By default, all users have access to these features.

11.3.2.1 To change display settings for BI launch pad

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*.

11.3.3 Managing Fiorified BI launch pad settings

This section walks you through how you can manage the following settings in the Fiorified BI launch pad:

- Configuring RESTful URL details in Central Management Console for logon to the Fiorified BI launch pad.
- Setting Authentication tab and CMS visibility in the Fiorified BI launch pad.
- Configuring email link for *Contact Administrator* option in the Fiorified BI launch pad.

11.3.3.1 Configuring RESTful URL details in CMC for logon to the Fiorified BI Launch Pad

After you install or upgrade BI 4.2 SP4, you need to configure RESTful Web Services URL for a user to be able to log on to the fiorified BI launch pad.

To configure RESTful Web Services URL details in CMC, perform the following steps:

1. Logon to the CMC, as an Administrator.
2. Navigate to *Manage* > *Applications* > *RESTful Web Services* > *Properties*.
3. Provide the WACS URL (hostname or fully qualified name where the WACS server is deployed).

11.3.3.2 Setting Authentication tab and CMS visibility in the Fiorified BI Launch Pad

To set Authentication tab and CMS visibility in the fiorified BI launch pad, perform the following:

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.

11.3.3.3 Configuring email link for Contact Administrator option in the Fiorified BI Launch Pad

To configure email link for the *Contact Administrator* option in the fiorified BI launch pad, perform the following

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.

11.3.4 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.

11.3.4.1 To modify display settings for Web Intelligence

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
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.
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.
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 capabalities. This code can be enabled or disabled in the Central Management Console, and fine-tuned using a white list to filter the on 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.

4. Click *Save & Close*.

> **Note**
>
> To revert your selection to the default display variables, click *Reset*.

11.3.5 Managing Central Management Console settings

In the *Applications* area of the CMC in BI platform, you can change the display options of Central Management Console by going to *Manage* > *Properties*.

For the Central Management Console, you can control:

- Processing extensions
- Processing settings
- Program object rights

11.3.5.1 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`

11.3.5.1.1 To enable or disable a type of program object

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*.

11.3.5.2 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.

> ℹ 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.

11.3.5.2.1 To register a processing extension with the system

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.

You can now select this processing extension to apply its logic to particular objects.

11.3.6 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.

> **i 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

> **i 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.

> **i 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.

11.3.6.1 Configuring a New BI Commentary Database

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.

To configure a new database for BI Commentary, proceed as follows:

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*.

   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.

   > **i** Note
   >
   > You need to restart all APS servers that host BI Commentary service for the changes to take effect.

You have now configured a new database to store comments from the BI Commentary application.

11.3.7 Managing Recycle Bin Settings

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

Only items in the public folder can be temporarily stored in the Recycle Bin.

11.3.7.1 Restoring an Item from the Recycle Bin

The Recycle Bin displays a list of deleted items. In order to restore an item from the recycle bin, proceed as follows:

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.

   > **i 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.

You have now successfully restored an item from the Recycle Bin.

11.3.7.2 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.

In order to permanently delete items from the Recycle Bin, proceed as follows:

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*.

You have now successfully deleted an item from the Recycle Bin.

Emptying the Recycle Bin

In order to empty the Recycle Bin, proceed as follows::

1. Log on to the CMC.
2. From the *Manage* pane on the CMC home page, choose *Recycle Bin*.
3. Choose *Empty Recycle Bin*.

You have now successfully emptied the Recycle Bin.

11.3.7.3 Enabling Auto-Cleanup for the Recycle Bin

You can run auto-cleanup of the recycle bin periodically.

To enable auto-cleanup of the recycle bin, proceed as follows:

1. Log on to the CMC.
2. From the *Manage* pane on the CMC home page, choose *Recycle Bin*.
3. From the *Recycle Bin* dialog box, choose *Properties*.

   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 *OK*.

You have now successfully enabled auto-cleanup for the Recycle Bin.

11.3.8 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 175]

11.3.8.1 To modify Alerting default properties

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.

Option	Description
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 194]

11.3.8.2 To modify alerting destination properties

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 175]
Managing alerting settings [page 194]

11.3.9 Managing widgets settings

Widgets for SAP BusinessObjects is a desktop application that allows users to add mini-applications to their desktop for easy access to business intelligence content on BI platform and Web Dynpro applications on SAP NetWeaver Application Servers.

From the "Applications" area of the CMC, you can control user access to create and use widgets on their desktops, as well as their ability to search the BI platform repository from within the widgets application on their desktop.

You can grant users or groups the ability to:

- Use widgets
- Edit objects created by widgets
- Modify user rights to access objects

> **i** Note
>
> By default, all general users have access to these features.

11.3.10 Managing SAP BusinessObjects Mobile settings

You can define which features your users have access to for SAP BusinessObjects Mobile by settings its properties and security rights from the Applications area of the CMC.

11.3.10.1 To modify SAP BusinessObjects Mobile default mobile properties

1. Go to the *Applications* area of the CMC.
2. Select *SAP BusinessObjects Mobile Application* and right click on this application.
3. Select *Properties*.
4. In the *Mobile Properties*, set the appropriate values for the following properties:

Property	Default Values	Description	Possible Values
`default.corporateCategory`	'Mobile'	Provide a name for a corporate category. Documents assigned to this category are mobile-ready documents. Mobile users can access the BI documents assigned to this category using an SAP BusinessObjects Mobile app on any mobile device (including Blackberry, Android and iOS). If there is more than one category name, specify the values, separating each with a comma. **i Note** The value specified here is case-sensitive.	Any specific corporate category chosen by the admininstrator.
`default.personalCategory`	'Mobile'	Provide a name for a personal category. Documents assigned to this category are personal to the user and cannot be accessed by other mobile users. If there is more than one category name, enter the values, separating each with a comma. **i Note** The value specified here is case sensitive.	Any specific personal category chosen by the admin.
`default.category.mobiledesigned`	'MobileDesigned'	Provide a name for a mobile designed category. Documents assigned to this category will appear in Page Layout mode when user view the documents on the mobile device. If there is more than one category	Any specific personal category chosen by the admin.

Property	Default Values	Description	Possible Values
		name, enter the values, separating each with a comma. **i Note** The value specified here is case sensitive.	
`default.category.secure`	'Confidential'	Provide a name for a secure category. Documents assigned to this category can be viewed by the user only in online mode. User cannot download or save a local copy of this document.If there is more than one category name, enter the values, separating each with a comma. **i Note** The value specified here is case sensitive.	Any specific personal category chosen by the admin.
`default.category.featured`	'Featured'	The value for this property is currently not used in the SAP BI app.	
`default.imageSize`	'1048576 bytes'	Specify the maximum size for an image that is displayed in the SAP BI app on a mobile device.	Any numeric value
`default.save.maxPages`	20	Specify the number of search results to be displayed per page on the mobile device.	Any numeric value

5. (Optional) To add a property, select *+Add More...* and enter the property details.
6. (Optional) To delete one or more properies, select the checkbox corresponding to the required property.
7. Click *Save & Close*.

11.3.10.2 To modify SAP BusinessObjects Mobile default client settings

1. Go to the *Applications* area of the CMC.
2. Select *SAP BusinessObjects Mobile Application* and right click on this application.
3. Select *Properties > Client Settings*.
4. In the *Client Settings*, set the appropriate values for the following properties:

Property	Default Values	Description	Possible Values
`savePassword`	'false'	Allows the mobile user to save password on the client application while creating connection. On selecting this option, the user is not to enter the password everytime he logs on to the application. To enable save password option on the client application, set the value as 'true'.	true or false
`offlineStorage`	'false'	Allows the mobile user to save a local copy of the document on your mobile device. To enable the user to save a local copy of the document, set the value to 'true'.	true or false
`offlineStorage.ttl`	'365'	Specify the maximum number of days after which the document will expire on the server.	Any numeric value
`offlineStorage.appPwd`	'true'	Allows the mobile user to enter application password while creating connection. To enable App password option on client application, set the value to 'true'.	true or false

5. (Optional) To add a property, select *+Add More...* and enter the property details.
6. (Optional) To delete one or more properies, select the checkbox corresponding to the required property.
7. Click *Save & Close*.

11.3.11 Managing Push Notifications service in SAP BusinessObjects Mobile

SAP BusinessObjects Mobile server pushes notifications to iOS devices of SAP BusinessObjects Mobile application users. Notifications are pushed in the following scenarios:

- When BI documents downloaded on a user's device have an update or a new instance available on the server.
- When a new document is received in user's BI Inbox.
- When the BI platform or the BOE administrator broadcasts a message.

Notifications are automatically pushed to the device from the Mobile server through Apple Push Notification Server (APNS). Users don't need to be connected to server receive push notifications. User can receive push notifications even when the app is not running on the system. "Notification settings" must be enabled in the application. For more information on configuring Push Notifications, refer *Mobile Server Deployment and Configuration Guide* for Mobile Server 4.2.

> **i** Note
>
> In order to enable push notifications in mobile, BIMobileService must be running in the APS.
>
> As BIMobileService does not consume large memory, you can run in along with other services in the APS.

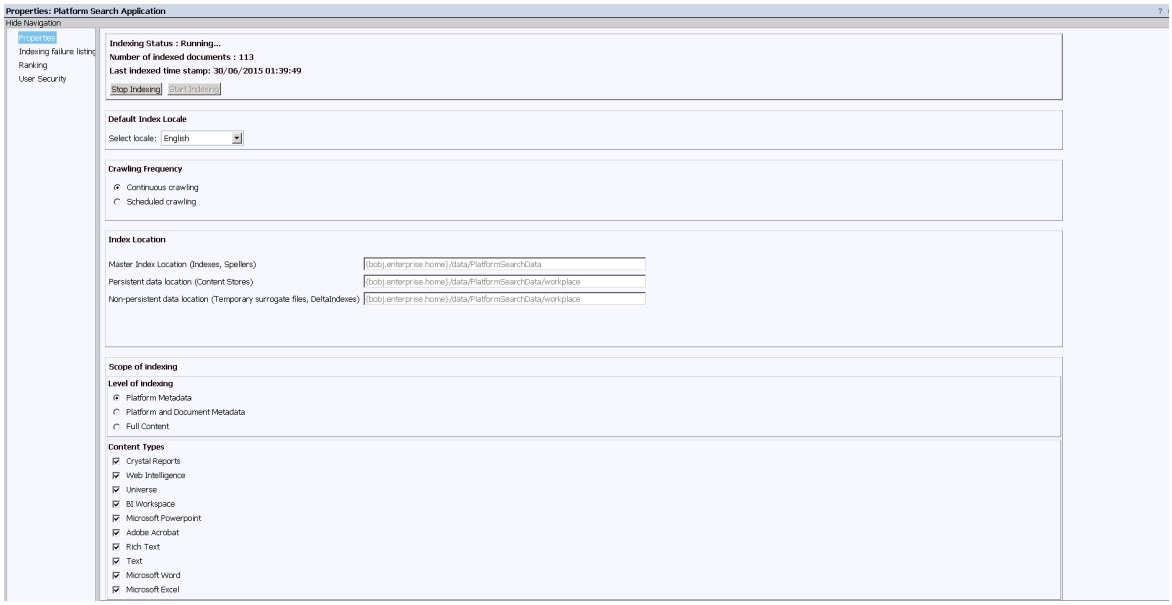
11.3.12 Managing Platform Search settings

In the *Applications* area of the CMC in the BI platform, you can specify system-level settings for the Platform Search application.

11.3.12.1 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*. **i 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. **i 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. **i 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 • Flash • Agnostic • Analytic • Hyperlink • Program • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset

Option	Description
	• VISI.Lums • VISILums • User • UserGroup

5. Click *Save & Close*.

> **i** 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.

11.3.12.2 Indexing Failure Listing

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 following steps:

1. Go to the *Applications* area of the CMC.
2. Select *Platform Search Application*.
3. Click *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.

11.3.13 Configuring BEx Web Integration

BEx Web applications are Web-based applications from the Business Explorer (BEx) of SAP Business Warehouse (BW) for data analysis, reporting, and analytical applications on the Web.

The Business Explorer is the SAP NetWeaver Business Intelligence suite, which provides flexible reporting and analysis tools for strategic analyses and decision-making support. These tools include query, reporting, and analysis functions. As an employee with access rights, you can evaluate historical or current data at various levels of detail and from different perspectives, both on the Web and in Microsoft Excel.

Users access the data from the SAP NetWeaver Portal or from the BI launch pad of SAP BI platform. Authors of BEx Web applications can execute the Web applications directly in the BI launch pad from BEx Web Application Designer.

To integrate BEx Web applications into the BI platform, perform the following configuration steps:

1. Set up a server for the BEx Web applications in the Central Management Console (CMC).

   You can use either a general or standalone server for the BEx Web applications.

   > → Tip
   >
   > We recommend setting up a standalone server for the BEx Web applications, as the general server is normally used by many other services.

2. Configure the server settings.
3. Check the connection to the BW system.
4. To ensure that authors can run BEx Web applications directly in the BI launch pad from BEx Web Application Designer, make the relevant settings in the *Connected Portals* table (**RSPOR_T_PORTAL**) in the BW system.

After the configuration of the BI platform server, users can open BEx Web applications in the BI launch pad. They can navigate in the data here and save the BEx Web applications as bookmarks in the web browser favorites.

> ! Restriction
>
> Integration is supported as of the following SAP NetWeaver releases:
>
> SAP NetWeaver 7.0 Enhancement Package 1 Support Package Stack 8
> SAP NetWeaver 7.3 Support Package Stack 1
>
> Because the SAP NetWeaver Java stack is not required for this integration, the following restrictions apply:
>
> Information Broadcasting is not supported.
> Because the portal and Knowledge Management of SAP NetWeaver are not needed, document integration and the use of portal motives are not supported in the BEx Web applications.
> The *Report* Web item is not supported. We recommend that you use SAP Crystal Reports for formatted reporting.
> To create print versions of BEx Web applications, the Export Library for SAP Business Explorer is used. Adobe Document Services (ADS) are not available.
> The BEx Web applications that are integrated into the BI platform can contain only data sources that are stored in the BW master system. In system administration, you define which system is configured as the BW master system in the BI platform.
> Single sign-on between the BI platform and the SAP NetWeaver BW system is not enabled. For each BI platform session, BEx Web applications users are requested to log on to the corresponding BW master system.
> Report-report interface from and to BEx Web applications is not supported. Corresponding commands won't be executed.
> Dashboards based on BEx queries or query views and created with SAP BusinessObjects Dashboards are not supported.

For more information about the features of BEx Web applications, see the SAP Help Portal at http://help.sap.com: *SAP NetWeaver 7.3* > *SAP NetWeaver Library: Function-Oriented View* > *Business Warehouse* > *SAP Business Explorer* > *BEx Web* > *Analysis & Reporting: BEx Web Applications*.

For more information about accessing and saving BEx Web applications in the BI launch pad, see the *BI Launch Pad User Guide* at http://help.sap.com.

Related Information

Starting a Server for BEx Web Applications [page 209]
Starting a Standalone Server for BEx Web Applications [page 209]
Configuring Server Settings [page 210]
Checking Connection to BW System [page 210]
Configuring a Connection Between BEx Web Application Designer and the BI platform [page 211]

11.3.13.1 Starting a Server for BEx Web Applications

Before you can perform this task, the Adaptive Processing Server must be in a Stopped state.

1. Log on to the Central Management Console (CMC).
2. Choose *Servers*.
3. Expand the *Service Categories* node, and choose *Analysis Services*.
4. Select *Adaptive Processing Server*, and choose *Select Services* in the context menu.
5. Move *BEx Web Applications Service* from the *Available Services* list to the Services list on the right side.
6. Restart the BEx Web Applications Service by restarting the Adaptive Processing Server.

11.3.13.2 Starting a Standalone Server for BEx Web Applications

1. Log on to the Central Management Console (CMC).
2. Choose *Servers*.
3. Expand the *Service Categories* node and choose *Analysis Services*.
4. Select the *Adaptive Processing Server* and choose *Clone Server* in the context menu.
5. Enter a name for the server (`AdaptiveProcessingServer` for example) and select the required node in the *Clone to Node* box.
6. Select the cloned server and choose *Select Services* in the context menu.
7. Select *BEx Web Applications Service* in the *Available Services* list and move it to the Services list on the right side.
8. Start the BEx Web Applications Service by starting the new Adaptive Processing Server.

11.3.13.3 Configuring Server Settings

1. Log on to the Central Management Console (CMC).
2. Choose *Servers*.
3. Expand the *Service Categories* node and choose *Analysis Services*.
4. Select the server that hosts the BEx Web Applications Service and choose *Properties* in the context menu.
5. Under the *BEx Web Applications Service Configuration* in the *BEx Web Applications Service* area, make the following settings:
   a. Check (and change if necessary) the maximum number of client sessions.
   b. Under *SAP BW Master System*, enter the name of the OLAP connection to the BW system that you created in the BI platform. The default name is *SAP_BW*.
   c. Enter the name of the *JCo Server RFC Destination* that you entered in the BW system under *Configuration of RFC Connections* (transaction code **sm59**).
   d. Enter the name of the *JCo Server Gateway Host* that you defined in the BW system under *Configuration of RFC Connections* (transaction code **sm59**).
   e. Enter the name of the *JCo Server Gateway Service* that you defined in the BW system under *Configuration of RFC Connections* (transaction code **sm59**).
   f. Check (and change if necessary) the *JCo Server Connection Count*.
6. Choose *Save & Close*.
7. Select the server that hosts the BEx Web Applications Service and choose *Restart Server* in the context menu.

   To apply the selected settings, you have to restart the server.

> **i Note**
>
> Before you restart the server, the RFC destination in the ABAP system must have been created.

Related Information

Creating an RFC destination in the ABAP System [page 212]

11.3.13.4 Checking Connection to BW System

1. Log on to the Central Management Console (CMC).
2. Choose *OLAP Connections*.
3. Check whether a connection has been established to the BW system. If not, click the *New connection* button to set one up. The default name of the connection is **SAP_BW**. You can also enter a different name.
4. Make sure that you have selected *Pre-defined* under *Authentication* and have made the required entries for user and password.

> **i Note**
>
> This user account is required for the JCo server RFC destination, which allows the integration of BEx Web Application Designer, the BW system, and the BI platform.

> **→ Tip**
>
> To make the connection secure, make sure that only administrators have access rights to it.
>
> 1. To do this, right-click the connection to the BW system (default name **SAP_BW**) and choose *User Security*.
> 2. Make the required security settings and give access rights only to administrators if possible.

11.3.13.5 Configuring a Connection Between BEx Web Application Designer and the BI platform

To ensure that authors can run BEx Web applications directly in the BI launch pad from BEx Web Application Designer, you need to make the relevant settings in the *Connected Portals* table (**RSPOR_T_PORTAL**) in the BW system.

1. In the BW system, call transaction **SM30** (*Table View Maintenance*).
2. Under *Table/View*, enter **RSPOR_T_PORTAL**.
3. Choose *Maintain*.
4. To create a new entry, choose *New Entries*.
5. Make the following settings:
   a. To ensure integration between the BW system and the BI platform, you have to create an RFC destination in transaction **SM59**. Enter this RFC destination under *Destination*.
   b. Select *Standard Portal*. This ensures that Web applications in Web Application Designer are always called in the BI platform.
   c. Under *URL Prefix*, enter the URL to the BI platform Web Application Container Server (WACS), including the protocol, host name and port, **http://<wacs><domain>:<port>** for example.
   d. Under *Platform*, select *BOE*.
   e. Select *Use SAP Export Lib (PDF)* if you want the Export Library for SAP Business Explorer to be activated, thus allowing PDF, PostScript and PCL files to be exported from BEx Web applications.
6. Save your entries.

Related Information

Creating an RFC destination in the ABAP System [page 212]

11.3.13.5.1 Creating an RFC destination in the ABAP System

To integrate the BW system and the BI platform, you need an RFC destination. This RFC destination allows the BW system and the BI platform to communicate with one another.

1. Call *Configuration of RFC Connections* (transaction code**SM59**).
2. Choose *Create*.
3. Maintain the RFC destination:
   a. Enter a name for the RFC destination.
   b. Select *T for TCP/IP connection* as the connection type.
   c. Enter a description.

      You can maintain the description of the RFC destination language dependently.
   d. Under *Technical Settings*, select *Registered Server Program* as the activation type.
   e. Under *Technical Settings*, enter the program ID.

      The program ID must be identical to the program ID (JCo Server RFC Destination) that you specified when creating the destination for this BW system in the BI platform server.
   f. Under *Technical Settings* under *Gateway Options*, enter the gateway host and the gateway service that the BI platform server uses to communicate with the BW system.
4. On the *Logon & Security* tab page, activate the *Send SAP Logon Ticket* option.
5. Save your entries.

Related Information

Configuring Server Settings [page 210]

11.3.14 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.

11.3.14.1 To create an SAP HANA connection

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.

If the `key.pem` file does not exist in the `.ssl` directory, then SAP HANA was not configured correctly to use SSL.

11.3.14.2 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.

> **i 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.

> **i 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.

11.3.14.3 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.
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.

11.3.15 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*.

11.3.16 Managing collaboration settings

11.3.16.1 Managing collaboration-application integration

This guide is intended for BI platform administrators who will integrate the BI platform with a SAP Jam collaboration application.

Use the *Applications* area of the Central Management Console (CMC) in the BI platform to enable and configure collaboration.

The following additional configuration is required in the collaboration application's Enterprise Agent:

- Establish an HTTPS connection with a service provider
- Fulfill prerequisites for authentication

After SAP Jam is configured, feeds from the collaboration application are available in the BI launch pad.

SAP Jam does not support Microsoft Internet Explorer 11.

11.3.16.1.1 Collaboration prerequisites

Collaboration prerequisites must be met before you integrate the BI platform with a collaboration application.

- The BI platform must be installed with at least one Central Management Server (CMS).
- The collaboration application (SAP Jam) must be configured in the Central Management Console (CMC).
- A collaboration application (SAP Jam) Enterprise organization must be defined.
- SAP Jam users must belong to the Enterprise organization.
- A SAP Jam Enterprise Agent is required to provision users who use an on-premise LDAP/AD directory service.

11.3.16.1.2 BI platform configuration

11.3.16.1.2.1 Collaboration configuration options

Collaboration options appear in the *Properties: Collaboration* dialog box in the Central Management Console (CMC) in the BI platform.

To access the *Properties: Collaboration* dialog box, on the *Applications* tab in the CMC, click *Collaboration*, and select *Manage* > *Properties*.

Option	Description
Enable Collaboration	Select this check box, and select *SAP Jam*.
Connection URL	Enter the URL to the collaboration application.
Unique Identity Provider ID	Enter a unique value for your BI platform deployment. The value should be associated with the certificate used to configure integration on the collaboration application's administration console. The application asserting an identity for single sign-on must be configured as an administrative OAuth application.
Identity Provider Base64 Certificate	When you click *Generate*, a certificate is created in this box. Use the certificate in the collaboration application's administration console to generate an OAuth Consumer Key. The certificate establishes the trust relationship between the collaboration application 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.
OAuth Consumer Key	Enter the OAuth Consumer Key that was generated from the collaboration application's administration console.
Connecting using proxy	Select this check box to enable connection through proxy, and enter information about the proxy host in the *HTTP Proxy Host* and *Port* boxes. To allow inbound connections from collaboration application servers to your corporate network, you must have a reverse proxy in the DMZ. To add a trusted certificate from an SSL certificate provider to the reverse proxy, you must have a domain or subdomain name for the reverse proxy.
HTTP Proxy Host	In the reverse proxy configuration, enter an external address that is accessible to the collaboration application. For example, use `https://<ReverseProxy>/`, where `<ReverseProxy>` is the domain or subdomain name of the reverse proxy. The collaboration application uses this address to send information to the BI platform. The reverse proxy uses this address to redirect information received from the collaboration application to the machine containing the collaboration application's Enterprise Agent.
Port	The collaboration application's Enterprise Agent is configured to listen from port 8443.

11.3.16.1.2.2 Enabling and configuring collaboration in the CMC

This task requires a valid connection to the collaboration application's (SAP Jam) administration console. You will need to pass and retrieve security details from the console.

For security reasons, the following default accounts cannot send or schedule content to SAP Jam:

- Guest
- SMAdmin
- Administrator
- WaaWSServletPrincipal

1. In the Central Management Console (CMC) in the BI platform, go to the *Applications* area, and double-click *Collaboration*.
2. In the *Properties: Collaboration* dialog box, select the *Enable Collaboration* check box, and select *SAP Jam*.
3. In the *Connection URL* box, enter the URL to the collaboration application.
4. In the *Unique Identity Provider ID* box, enter a unique identity provider value for your BI platform deployment.

   Make a note of the identity provider value; you will use it to configure the collaboration application.
5. Click *Generate* (or *Regenerate*, if a certificate has been created before).
   The certificate appears in the *Identity Provider Base64 Certificate* box. You will use the certificate to configure the collaboration application.
6. In the *OAuth Consumer Key* box, enter a valid OAuth Consumer Key.
7. If you are connecting via proxy to the server running SAP Jam, perform the following actions:
   a. Select the *Connecting using proxy* check box.
   b. In the *HTTP Proxy Host* box, enter the proxy host name of the server.
   c. In the *Port* box, enter the port number of the server.
8. Click *Save & Close*.

11.3.16.1.3 SAP Jam configuration

11.3.16.1.3.1 Registering a new SAML trusted IDP for SAP

You must register each user with a unique email address that corresponds to the user's Enterprise email address in the BI launch pad. The email addresses will be mapped between the BI platform and SAP.

Before you can register a new SAML trusted IDP:

- Your company must be added to and configured in SAP.
- You must have a valid SAP user account that is associated with your company in SAP.
- You must have company administration rights for your company in SAP and full administrator rights to the BI platform and the BI launch pad.
- The BI launch pad must be registered as an OAuth client that acts as a representative of the launch pad within SAP.

SAP Jam does not support Microsoft Internet Explorer 11.

1. In the upper-right corner of the Central Management Console (CMC) in the BI platform, select *Administrator* and then select *Admin*.
   Information about your company, including your SAP license, is displayed. Write down or otherwise make note of the information.
2. From the *Admin* menu, select *SAML Trusted ID's*, and click *Register your identity provider*.

   You must register the IDP that you created in the BI launch pad.

3. In the *IDP ID* box, enter the unique identity provider value that was created when SAP was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

   For example, enter **<CompanyName>_<SystemId>_<client>**
4. In the *Single Sign-On URL* box, enter the URL that directly accesses SAP.

   SAP uses this URL for single sign-on with the unique identity provider.
5. In the *Single Log-Out URL* box, enter the URL to display after logging off SAP.

   SAP uses this URL for single log-out with the unique identity provider.
6. In the *Default Name ID Format* box, enter the name ID format to use in authentication requests.
7. In the *Default Name ID Policy SP Name Qualifier* box, enter the SP name qualifier to use in authentication requests.
8. In the *Allowed Assertion Scope* list, select *Users in my company*.

   This option specifies the set of users for which SAP will accept assertions from the IDP.
9. In the *X509 Certificate (Base64)* box, enter the Base64 certificate value that was generated when SAP was configured in the BI platform.

   If you do not have the value, contact your external application administrator.
10. Click *Register*.

11.3.16.1.3.2 Creating an OAuth client for SAP Jam

Before you can create an OAuth Consumer Key:

- Your company must be added to and configured in SAP Jam.
- You must have a valid SAP Jam user account that is associated with your company in SAP Jam.
- You must have company administration rights for your company in SAP Jam and full administrator rights in the BI platform and in the BI launch pad.
- The BI launch pad must be registered with SAP Jam as an OAuth client, which acts as a representative of the launch pad within SAP Jam.
- Each user must be registered in SAP Jam with a unique email address that corresponds to the user's Enterprise email address in the BI launch pad. The email addresses will be mapped between the BI platform and SAP Jam.

SAP Jam does not support Microsoft Internet Explorer 11.

1. In SAP Jam, from the *Administrator* menu in the upper-right corner, select *Admin*.
   Information about your company, including your SAP Jam license, appears.
2. From the *Admin* menu, select *OAuth Clients*, and click *Add OAuth Client*.
3. In the *Register a new OAuth Client* dialog box, in the *Name* box, enter the unique identity provider value that was created when SAP Jam was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

   SAP Jam displays the application name as a hyperlink (to the URL you enter) when it takes action on behalf of a user.

   For example, enter **<CompanyName>_<SystemId>_<Client>_<Application>**

4. In the *Integration URL* box, enter the URL for the BI launch pad.

   SAP Jam displays the application name as a hyperlink to the URL when it takes action on behalf of a user.
5. In the *X509 Certificate (Base64)* box, enter the Base64 certificate value that was generated when SAP Jam was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

   If you leave this box blank, SAP Jam supplies a consumer secret.
6. Click *Save*.

The OAuth Consumer Key is generated. Make a note of the OAuth Consumer Key value for the BI platform administrator to use.

11.3.17 Managing discussion settings

In the *Applications* area of the CMC in the BI platform, you can specify system-level settings for discussion threads.

For the *Discussions* application you can manage and interact with discussion threads in several ways, including:

- Searching for discussion threads according to specified search criteria.
- Sorting discussion thread search results.
- Deleting discussion threads.

> **i** Note
>
> User rights settings are not available for the Discussions application. However, you can set rights on individual reports.

11.3.17.1 To search for a discussion thread

By default, the *Discussions* page displays the titles of all discussion threads. Only the root level threads are displayed.

To page through the list of discussion threads, use the Previous and Next buttons. You can also search for a specific thread or group of threads.

1. Go to the *Applications* area of the CMC and select *Discussions*.
2. Click *Manage* > *Manage Threads*.
   The *Notes Administration* dialog box appears.
3. In the *Field name* list, select an option.

Option	Description
Thread title	Searches by thread title.
Creation date	Searches by creation date.

Option	Description
Last modified date	Searches by the last date modified.
Author	Searches by author.

4. On the second list, refine your search.

> **i Note**
>
> Searches are not case-sensitive.

- If you chose *Thread title* or *Author*, choose from the following options in the second field.

Option	Description
is	Searches for discussion threads where the thread title, or the author name, exactly match the text you type into the third field.
is not	Searches for discussion threads where the thread title, or the author name, do not exactly match the text that you type into the third field.
contains	Searches for discussion threads that contain the search text string within any part of the thread title or the author's name.
does not contain	Searches for discussion threads that do not contain the text string within any part of the thread title.

- If you chose *Creation date* or *Last modified date*, choose one of the following options, and then specify a search date.

Option	Description
before	Searches for discussion threads that were created or modified before the search date.
after	Searches for discussion threads that were created or modified after the search date.
between	Searches for discussion threads that were created or modified between the two search dates.

5. To further refine your search, use the third text field.
   - If you selected a text-based search in the first two fields, type in the text string.
   - If you chose a date-based search, enter the date or dates in the appropriate fields.
6. Click *Search*.

11.3.17.2 To sort your discussion thread search results

When you search discussion threads, you can select how you want your search results to display. For example, you can sort them in ascending alphabetical order, and choose the number of results to display per page.

1. Go to the *Applications* area of the CMC and select *Discussions*.
2. Click *Manage* > *Manage Threads*.
   The *Notes Administration* dialog box appears.
3. In the *Sort by* list, select a sort option.

Option	Description
Thread title	Sort by the title of a discussion thread.
Creation date	Sort by the date the discussion thread was created.
Last modified date	Sort based on the date a discussion thread was last modified.
Author	Sort by the author of a specific discussion thread.

4. In the second list, select if you want the records to be displayed in ascending or descending order.
5. In the third text field, enter how many discussion thread results you want displayed on each page.
   The default is 10 results per page.
6. Click *Search*.

11.3.17.3 To delete a discussion thread

You can delete any discussion thread in the *Applications* area of the CMC in the BI platform.

1. Go to the *Applications* area of the CMC and select *Discussions*.
2. Click *Manage* > *Manage Threads*.
   The *Notes Administration* dialog box appears.
3. In the results list, search for the discussion thread you want to delete and select it.
4. Click *Delete*.

12 Managing Data Sources and Connections

12.1 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, username, 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:

- The universe design tool: connections are stored in the repository.
- The information design tool: connections can be created locally and then published to the repository, or created and edited directly in the repository.

> **i** Note
>
> For information on how to manage OLAP data source connections, see the *SAP BusinessObjects Analysis, edition for OLAP Administrator Guide*.

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 47]
Connection rights [page 432]

12.1.1 To delete a universe connection

> **→** Tip
>
> It is also possible to delete connections in the universe design tool and the information design tool.

1. In the *Connections* area, select a universe connection from the list.
2. Click *Manage* > *Delete*.

12.2 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 tools:

- The universe design tool. Universes created with this tool can be distinguished by the .unv extension and are therefore called .unv universes. The .unv universes are defined on a secured connection and stored in the repository Universes folder.
- 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 47]
Universe design tool [page 437]
Universe (.unv) rights [page 428]
Information design tool [page 437]
Universe (.unx) rights [page 429]

12.2.1 To delete universes

> → Tip
>
> It is also possible to delete universes in the information design tool.

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*.

13 Managing Hot Backups

13.1 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.

> **i 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.

> **i 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).

> **i 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.

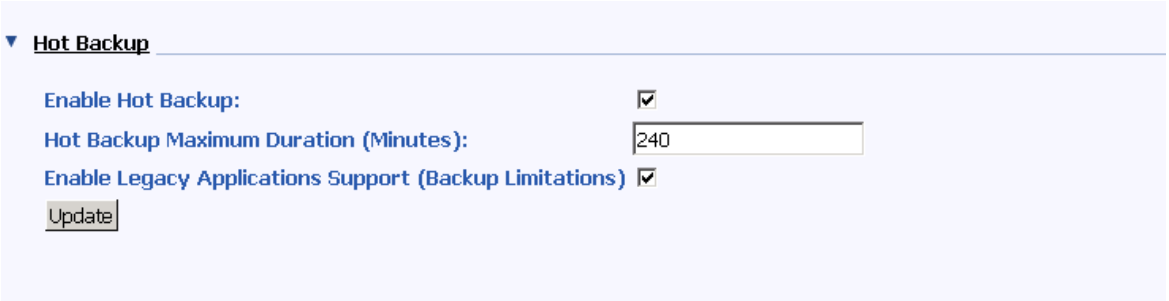
13.1.1 To enable hot backups

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.

   > **i 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.



Once hot backup support is enabled, you can perform backups using your database and file system vendor's backup tools.

14 Folders

14.1 Folders

Folders are objects used to group and organize other objects so that content is separated into logical groups. Each object in the BI platform must reside in a folder.

By default, new objects that you add to a folder inherit the object rights of the folder. Because you can set security at the folder level, you can use folders to control access to information.

It is a good practice to set up folders in a structure that already exists in your organization (such as departments, regions, or your database table) and then use categories to set up an alternate system of organization.

14.1.1 Creating a folder

Before creating a new top-level (parent) folder, confirm that you are viewing *All Folders*.

To quickly edit the name, description, or keywords for a folder, select the folder, and select *Manage* > *Properties*.

1. Go to the *Folders* management area of the CMC.
2. Go the location where you want to create a folder.
   If you are creating a subfolder, locate the target folder in which to put the new folder.
3. Select *Manage* > *New* > *Folder*.
4. In the *Create Folder* dialog box, enter a name for the new folder, and click *OK*.

The new folder appears in the list of folders and objects.

You can add objects to the folder or edit the folder properties.

14.1.2 Deleting a folder

1. Go to the *Folders* management area of the CMC.
2. Locate and select the folder to delete.
   To simultaneously delete several folders, hold down the CTRL key or the SHIFT key, and click each folder to delete.
3. Select *Manage* > *Delete*.
4. In the *Delete* message box that appears, click *OK* to confirm the deletion.

The folder, all subfolders, reports, and other objects in the folder are removed from the BI platform.

14.1.3 Copying or moving a folder

1. Go to the *Folders* management area of the CMC.
2. Select the folder to copy or to move.

   If a folder is not at the top level, locate its parent folder, and select the parent folder's contents. To simultaneously copy or move several folders, hold down the CTRL key or the SHIFT key, and click each folder to copy or to move.
3. Select *Organize* > *Copy To* or *Organize* > *Move To*.
4. In the *Copy To* or *Move To* dialog box, select the destination folder.
5. Click *Copy* or *Move*.

The folder you selected is copied or is moved to the new destination.

14.1.4 Limiting report instances at the folder level

Setting limits enables you to automatically delete report instances in the BI platform.

The limits you set on a folder affect all objects in the folder. At the folder level, you can set limits for:

- The number of instances for each object, user, or user group
- The number of days that instances are retained for a user or a group

1. Go to the *Folders* management area of the CMC.
2. Locate and select the folder for which to set limits, and select *Actions* > *Limits*.
3. In the *Limits* dialog box, select the *Delete excess instances when there are more than N instances of an object* check box, and enter the maximum number of instances per object the folder can contain before instances are deleted in the box.

   The default value is 100.
4. Click *Update*.
5. To limit the number of instances per user or group, beside *Delete excess instances for the following users/groups*, click *Add*.
6. Select a user or a group, click > to add the user or group to the *Selected users/groups* list, and click *OK*.
7. For each user or group you added in step 6, in the *Maximum instance count per object per user* box, type the maximum number of instances you want to appear in the BI platform.

   The default value is 100.
8. To limit the age of instances per user or group, beside *Delete instances after N days for the following users/groups*, click *Add*.
9. Select a user or a group, click > to add the user or group to the *Selected users/groups* list, and click *OK*.
10. For each user or group you added in step 9, in the *Maximum instance age in days* box, type the maximum age for instances before they are removed from the BI platform.

    The default value is 100.
11. Click *Update*.

Related Information

Setting limits for instances [page 268]

14.1.5 Limiting documents in Inboxes

Setting limits enables you to automatically delete documents in the BI platform.

The limits you set on an inbox affect all objects in the inbox. At the inboxes level, you can set limits for:

- The number of documents for each inbox, user, or user group
- The number of days that documents are retained for a user or a group

1. Go to the *Inboxes* management area of the CMC.
2. Right-click on *Inboxes* and select *Limits*.
3. In the *Limits* dialog box, select the *Delete excess documents when there are more than N documents:* check box, and enter the maximum number of documents the inbox can contain before documents are deleted in the box.

   The default value is 100.
4. Choose *Update*.
5. To limit the number of documents per user or group, beside *Delete excess documents for the following users/groups* , choose *Add*.
6. Select a user or a group, click > to add the user or group to the *Selected users/groups* list, and click *OK*.
7. For each user or group you added in step 6, in the *Maximum document count* box, type the maximum number of documents you want to appear in the BI platform.

   The default value is 100.
8. To limit the age of instances per user or group, beside *Delete documents after N days for the following users/groups*, choose *Add*.
9. Select a user or a group, click > to add the user or group to the *Selected users/groups* list, and click *OK*.
10. For each user or group you added in step 9, in the *Maximum document count per user* box, type the maximum number of days for documents before they are removed from the BI platform.

    The default value is 100.
11. Choose *Update*.

15 Categories

15.1 Working with categories

15.1.1 Creating a category

1. In the CMC, select the *Categories* area.
2. Select *Manage* > *New* > *Category*.
3. In the *Create Category* dialog box, enter a name for the category in the *Enter a new category name* box.
4. Click *OK*.

The category is added to the BI platform.

15.1.2 Deleting a category

When you delete a category, all subcategories in it are deleted. However, reports and other objects in the category are not deleted from the BI platform.

1. In the CMC, select the *Categories* area.
2. Select the category to delete.

   If a category is not at the top level, locate the parent category and then the subcategory. To simultaneously delete several categories, hold down the CTRL key or the SHIFT key, and click each category to delete.
3. Select *Manage* > *Delete*.
4. In the *Delete* message box that appears, click *OK* to confirm the deletion.

The category is deleted from the BI platform.

15.1.3 Moving a category

When you move a category, the category retains the objects associated with it and its object rights.

For example, you have a South American Sales category that is accessible only to people in that region and a World Sales category containing worldwide sales reports that is accessible to all people. You move the region categories to the World Sales category. The South American Sales category retains its rights and associated objects, even though it is a subcategory of the World Sales category.

1. In the CMC, select the *Categories* area.

2. Select the category to move.

   If a category is not at the top level, locate its parent category and then the subcategory. To simultaneously move several categories, hold down the CTRL key or the SHIFT key, and click each category to move.

3. Select *Organize* > *Move To*.

   If there are many categories in the BI platform, enter the category name in the *Search title* box—or click *Previous*, *Next*, or + (plus sign) to browse the category list.

4. In the *Move To* dialog box, select the destination category, and click *Move*.

The category is moved to the new destination.

15.1.4 Adding an object to a category

1. In the CMC, select the *Folders* area.
2. Locate and select the object to add to a category.
3. Select *Manage* > *Categories*.
4. In the *Categories* dialog box, select the category to which to add the object.
5. Click *Save & Close*.

The object is added to the category.

15.1.5 Removing or deleting objects from a category

When you remove an object, you remove it from the category but the object remains in the BI platform. When you delete an object, you remove it from the category and delete it from the platform.

1. In the CMC, select the *Categories* or *Personal Categories* area.
2. Double-click the category from which to remove or to delete an object.
3. Select the object(s) to remove or to delete.
4. Perform one of the following actions:
   - Select *Actions* > *Remove From Category* to remove the object from the category but not from the platform.
   - Select *Manage* > *Delete* to remove the object from the category and delete it from the platform.
5. In the *Remove from Category* or *Delete* dialog box, click *OK* to confirm the removal or deletion.

The object is removed or deleted.

15.1.6 Viewing a user's personal categories

If you have the appropriate access rights, you can view, edit, and delete personal categories for users.

1. In the CMC, select the *Categories* area.

2. Select the user account for which to view personal categories.

A list of the user's personal categories appears.

15.1.7 Adding multiple objects to a category

1. Go to the *Categories* or *Personal Categories* management area of the CMC.
2. Locate and select the category to which you want to add objects.
3. Select *Actions* > *Add to Category*.
4. In the *Add to Category* dialog box, under *Available Objects*, locate the objects to add, and click to move the objects to the *Selected Objects* list.
5. Click *OK*.

16 Object Management

16.1 Default settings

Default settings let you edit and manage custom properties for various content objects. Depending on the object type, the default settings available may vary. This section lists the different types of default settings available and provides links to other topics for more information. The default settings are listed alphabetically.

Component Failure

This setting applies to object packages only.

Destinations

This setting only applies to objects that can be sent.

Events

This setting only applies to objects that can be scheduled and works in the same way as the event settings for scheduling.

Fallback Server(s)

In the *Properties: New Event* window, in *Event Settings*, the *Fallback Server(s)* field is introduced as a back up for the existing *Server* option to address the *Failover support for Event Server with File Events*.

The *Fallback Server(s)* list supports each event along with the existing *Server* option to select the default Event Server.

For example, if the default event server is down, then any event server from the fallback list can process the File Event as expected.

This option is available in both *Create* and *Edit File Event* scenarios.

Notification

This setting only applies to objects that can be scheduled and works in the same way as the notification settings for scheduling.

Program Logon

This setting applies to program objects only.

Program Parameters

This setting applies to program objects only.

Recurrence

This setting only applies to objects that can be scheduled and works in the same way as the recurrence settings for scheduling.

Schedule For

This setting only applies to objects that can be scheduled and works in the same way as the *Schedule For* settings for scheduling.

Scheduling Server Group

This setting only applies to objects that can be scheduled and works in the same way as the event settings for scheduling.

Related Information

To set component failure options for an object package [page 252]
To send an object or an instance to a destination [page 239]
Scheduling an object based on an event [page 261]

Scheduling an object to trigger an event [page 262]
Configuring success or failure notification for an instance [page 262]
Specifying a user account for a program object [page 251]
Specifying command-line arguments [page 248]
Setting the working directory for a program object [page 248]
Specifying the path to external or auxiliary files [page 249]
Specifying required parameters for Java programs [page 250]
Providing Java programs with access to other files [page 250]
Recurrence patterns [page 254]
Run Options for Recurrence Patterns [page 255]
Scheduling a report object for individual users [page 264]
Selecting a server or server group for a scheduled object [page 265]

16.2 Adding an object in the CMC

You must have administrative rights before you can add an object in the CMC.

1. Go to the *Folders* management area of the CMC.
2. Locate and select the folder to which to add an object.
3. Select *Manage* > *Add* , and select one of the following options:

Option	Description
Program File	Adds a program object
Local Document	Adds other types of objects

A dialog box appears, where you can specify the properties of the object.

4. Specify the properties of the object.
   The properties fields that appear vary according to the type of object that you chose to publish. The properties fields are summarized in the table "Object properties in the CMC".
5. To assign the object to a category, select the category in the list.
6. Click *OK*.
   The dialog box closes, and the CMC refreshes to display the object and the other contents of the folder.

16.3 To copy an object

1. In the *Folders* area, browse for the object that you want to copy and select it.
2. Click *Organize* > *Copy To* .
   The *Copy* dialog box appears.

3. In the *Select destination(s)* area, browse for the destination folder you want to copy the object to, and click > to move it to the *Destinations* list.

   > **i Note**
   >
   > In order to move the destination folder, you must select that folder in the details pane on the right.

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

4. When you are finished, click *Copy*.
   The object you selected is copied to the destination.

16.4 To move an object

1. In the *Folders* area, browse for the object you want to move and select it.
2. Click *Organize* > *Move To*.
   The *Move* dialog box appears.
3. Select the destination folder.

   > **i Note**
   >
   > In order to move the destination folder, you must select that folder in the details pane on the right.

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

4. Click *Move*.
   The object moves from the origin folder to the destination folder.

16.5 To create an object shortcut

Shortcuts are useful for granting a user access to an object without giving that user access to the entire folder in which the object is located.

After you create the shortcut, users who have access to the folder where the shortcut is located can access this object and its instances.

1. In the *Folders* area, browse for the object that you want to create a shortcut for and select it.
2. Click *Organize* > *Create Shortcut In*.
   The *Create Shortcut In* dialog box appears.
3. In the *Select destination(s)* area, browse for the folder you want to create a shortcut in, and click > to move the folder to the *Destinations* list.

> **Note**
>
> In order to move the destination folder, you must select that folder in the details pane on the right.

4. Click *Create Shortcut*.
   A shortcut to the object appears in the folder you specified.

16.6 To delete an object

You can delete one or more objects, a folder (which deletes all objects and instances in that folder), or object instances (rather than the object itself).

> **Note**
>
> When you delete an object, all of its existing instances and scheduled instances will be deleted.

1. Go to the *Folders* management area of the CMC.
2. Select the object that you want to delete.
3. Click *Manage* > *Delete*.
4. When you are prompted by a confirmation message, click *OK*.

16.7 To search for an object or objects

The search feature enables you to search for specific text within object titles or descriptions.

1. Go to the *Folders* management area of the CMC.

   The Search field is located in the upper right corner of the *Folders* management area. The search type is set to *Search title* by default.
2. Specify the search criteria.
   a. If you want to search by something other than the file name, click *Search title* to change the search type.

      Your options are:

      - *Search all fields*
        This option searches file names, keywords, and descriptions associated with objects.
      - *Search title*
        This option is the default option and searches file names.
      - *Search keyword*
        This option searches the keywords that are associated with objects.
      - *Search description*
        This option searches the descriptions that are associated with objects.

   b. Enter the text that you want to search for in the Search field.

3. Click *Search*.
   When the search is finished, a list of results that match your search criteria appears.

16.8 To send an object or an instance to a destination

You can send either a copy of an object or instance, or a shortcut to the object or instance. You can also select the destination, for example, FTP, SFTP, or BI Inbox. Not all types of objects can be sent to all destinations.

> **i Note**
>
> You can use *Organize* > *Send* to send existing objects or instances of an object to different destinations. The *Send* command handles existing objects or instances only. It does not cause the system to run the object and create new instances, nor does it refresh the data for a report instance.

1. Go to the *Folders* management area of the CMC.
2. Select the object or instance that you want to send.
   - If you want to send an object, select it, click *Organize* > *Send* and choose a destination.
   - If you want to send an instance, select the object and click *Actions* > *History*. In the *History* dialog box, select an instance, click *Send*, and click the destination option that you want.
     Select only instances with a status of Success or Failed. Instances with a status of Recurring or Pending are scheduled and do not contain any data yet.

Destination option	Description
BI Inbox	Sends the object to a user's BI launch pad inbox.
Email	Sends the object to a user's email address.
FTP Location	Sends the object to an FTP server location.
SFTP Location	Sends the object to an SFTP server location.
File Location	Sends the object to a local disk location.

> **i Note**
>
> Send Interactive Analysis documents to BI Inboxes only, or to an Email destination configured within Information platform services.

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

3. Configure your destination option.

   You can choose to use the Adaptive Job Server's default settings or your own settings. If you use your own settings, you can specify:

   - The users and groups who receive the object (if sent to a BI Inbox or an Email destination).
   - Whether to send a copy of the object or a shortcut that links to the object.
   - The name of the object that is sent.

- Whether to clean up instances after objects have been sent.
- The settings specific to the destination type (for example, a directory for the file location, or the host name and connection port for the FTP or the SFTP server).

4. When you are finished, click *Send*.

16.9 To change the properties of an object

1. In the *Folders* management area of the CMC, select an object.
2. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
3. Make your changes.

   You can change the object name, keywords, and description.
4. When you are finished, click *Save & Close*.

16.10 To check the relationships of an object

1. Navigate to the object for which you would like to run the relationship query.
2. Click *Manage* > *Tools* > *Check Relationships*.

   The *Query Results* area with the results of your relationship query is displayed.

   > → Tip
   >
   > As required, perform further checks on the relations of result objects by selecting an object and choosing *Manage* > *Tools* > *Check Relationships*.
3. To navigate back to your original query, select the name of the object from the Tree panel.

16.11 To create a new hyperlink

1. In the *Folders* or *Personal Folders* area, navigate to the folder in which you want to create a new hyperlink.
2. Click *Manage* > *New* > *Hyperlink*.
   The *Hyperlink* dialog box appears.
3. Enter a title, description, and keywords for your hyperlink.
4. In the navigation pane, click *URL*.
5. In the *URL* field, enter the URL.
6. Click *OK*.

17 Reports

17.1 Selecting refresh options for a report

You can select refresh options only in Crystal reports.

> → Tip
>
> You can click *Refresh report* to immediately refresh the report.

1. Go to the *Folders* management area of the CMC.
2. Select a report, and select *Actions* > *Refresh Options*.
3. In the *Refresh Options* dialog box, select the report elements to refresh from the source `.rpt` file.
4. Click *Update*.

17.2 Selecting report viewing options for a Crystal report

1. Go to the *Folders* management area of the CMC.
2. Locate and select the report for which to set viewing options.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Viewing Server Group* in the navigation list.
5. Under *Data refresh for viewing*, select *Use report specific viewing settings*, and select options for the report.
6. Click *Save & Close*.

17.3 Selecting default servers for processing an object

1. Go to the *Folders* management area of the CMC.
2. Select the report object for which to specify default servers.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, perform one of the following actions:
   - To specify the default servers for scheduling a report object, click *Scheduling Server Group* in the navigation list.
   - To specify the default servers for processing an object when you view it, click *Viewing Server Group* in the navigation list if the object is a Crystal report or *Web Intelligence Process Settings* if the object is a Web Intelligence document.

5. Click *Save & Close*.

17.4 Changing database settings in Crystal reports

You can select the database type, set default database logon information, view the data source or data sources for a Crystal report object and its instances, and optionally prompt users for a logon name and password when viewing a Crystal report instance.

If you select multiple report objects to change database settings, only the report objects with the same data source connection are updated. For information about supported databases and drivers, see the supported platforms documents on the SAP Service Marketplace.

1. Go to the *Folders* management area of the CMC.
2. Select the report object for which to change the database settings.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Database Configuration* in the navigation list.
5. Perform one of the following actions:
   - Select *Use original database logon information from the report*, and enter a user name and password for the original report database.
   - Select *Use custom database logon information specified here*, and enter a server name (or a DSN for an ODBC data source), database name, user name, and password for predefined database drivers or for a custom database driver. If you changed the default table prefix in your database, specify a custom table prefix.
6. Perform one of the following actions:
   - To prompt users for a password when they refresh a report, select *Prompt the user for database logon*. The BI platform prompts users the first time they refresh a report. When users refresh the report again, they are not prompted. This option does not effect scheduled instances.
   - To use the user's logon and password to log on to the database, select *Use SSO context for database logon*.
     The BI platform must be configured for end-to-end single sign-on or for single sign-on to the database. For more information, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
   - To use the same database logon information that was used when the report ran on the job server, select *Use same database logon as when report is run*.
   - To use the database credentials specified for the user account, select *Use user database credentials for database logon*.
7. Click *Save & Close*.

17.5 Updating default parameter values for a Crystal report

When a Crystal report contains parameters, you can set the default value for each parameter. The default values are used when a report instance is generated.

Parameter fields (with preset values) enable users to view and to specify which data appears in the BI platform. Using a BI platform application such as the BI launch pad, your users can open a report with the default value(s) or choose other value(s). If you do not specify a default value, users are prompted for a value when scheduling a report.

1. Go to the *Folders* management area of the CMC.
2. Select a Crystal report object for which to update the default prompt values.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Prompts* in the navigation list.

   This option is available only if a report object contains parameters. If it does not contain parameters, this option is not available; skip this step.
5. In the *Default Value* column, type or select a default value for the parameter.

   Options appear for changing the default value. Depending on the parameter value type, you can type a value in the box or choose a value in a list.
6. Click the *Clear Value* button to clear the current value set for the parameter.
7. Select the *Prompt when viewing* check box to prompt users before they can view a report instance in a BI platform application.
8. Click *Save & Close*.

17.6 Updating prompts for a Web Intelligence document

When a report contains parameters, you can set the default prompt value for each parameter. The default value is used when a report instance is generated.

Prompt fields (with preset values) enable users to specify which data they see. Through an application in the BI platform, such as the BI launch pad, users can either use the report with the preset default value(s) or choose other value(s). If you do not specify a default value, users are prompted for a value when scheduling a report.

1. Go to the *Folders* management area of the CMC.
2. Select a Web Intelligence document for which to update prompts.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Prompts* in the navigation list.

   This option appears only if the Web Intelligence document object contains prompts. If it does not contain prompts, this option is not available.
5. Click *Modify*.
6. Select a prompt, and enter a value for it.

   If the available values do not appear, click the *Refresh Values* button.
7. Repeat steps 5 and 6 for each prompt value you want to change.

8. Click *Apply*, and click *Save & Close*.

Related Information

Updating default parameter values for a Crystal report [page 243]

17.7 Using filters

You can use filters for only some types of reports. For example, you cannot use them with Web Intelligence documents, SAP Crystal reports in `.rptr` format, or reports created in SAP Crystal Reports for Enterprise.

1. Go to the *Folders* management area of the CMC.
2. Select the report object for which to add filters.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Filters* in the navigation list.
5. To update or add new selection formulas, perform one of the following actions:
   - In the *Record selection* box, create or edit one or more record selection formulas that limit the records used when a report is scheduled.
   - In the *Group selection* box, create or edit one or more group selection formulas that limit the groups used when a report is scheduled.
6. Click *Save & Close*.

17.8 Selecting a printer for Crystal reports

1. Go to the *Folders* management area of the CMC.
2. Select the report object to assign a printer to.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Print Settings* in the navigation list.
5. Under *Print Settings*, select the *Print Crystal reports when scheduling* check box.

   Crystal reports will be sent to the printer in SAP Crystal Reports format, which does not interfere with the page layout you selected when scheduling the report.
6. In the *Number of Copies* box, enter the number of copies to print.
7. Under *Page Range*, select *All* to print all report pages, or select *Pages* and enter the first and last pages to print in the boxes.
8. In the *Set collate option to* list, perform one of the following actions:
   - Select *Collate* to collate the report.

- Select *Do not collate* if you do not want to collate the report.
- Select *Use printer defaults* to use the default collation setting of the printer.

9. In the *Page Scaling* list, perform one of the following actions:
   - Select *Scale to fit* to proportionately scale the report page to fit the printed page.
   - Select *Only shrink to fit* to shrink the report page to fit the printed page.
   - Select *Do not scale* if you do not want to scale the report.
10. Select the *Center the page* check box to center the report on the printed page.
11. Select the *Fit horizontal pages into one page* check box to fit horizontal pages on one printed page.
12. Under *Specify page layout*, perform one of the following actions:
    - Select *Default printer* to print to the Crystal Reports Job Server's default printer.
    - Select *Specify a printer*, and enter the printer's path and name in the box.
      If your job server is on Windows, enter **`\\<PrintServer>\<PrinterName>`**, where `<PrintServer>` is the name of the printer server and `<PrinterName>` is the name of the printer.
      If your job server is on Unix, confirm that the Unix printer is shown (not hidden), and enter the print command you normally use, such as `lp -d <PrinterName>`.
13. Click *Save & Close*.

17.9 Selecting page layout options for Crystal report and PDF objects

1. Go to the *Folders* management area of the CMC.
2. Select the report object for which to set the page layout.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Print Settings* in the navigation list.
5. Under *Print Settings*, to select the default print mode, perform one of the following actions:
   - Select *Always print to PDF (Preview)* to use PDF print settings when printing the report from a web viewer.
   - Select *Follow Crystal Reports preference setting* to use the default Crystal report print settings defined in the CMC preferences.
6. Under *Specify page layout*, in the *Set layout to* list, perform one of the following actions:
   - Select *Report file default* to use the page layout defined in Crystal Reports.
   - Select *Specify printer settings* to use the printer's default page layout, and select the Crystal Reports Job Server default printer or a different printer.
     You can print scheduled report instances only to the printer specified under *Print when scheduling*. That is, you cannot set a report to use the default page layout of one printer and then print to a different printer.
   - Select *Custom settings* to customize all page layout settings, and select the page orientation and page size.
7. Click *Save & Close*.

17.10 Assigning a processing extension to a report

You can apply more than one processing extension to a report object.

Before you can apply a processing extension to a report object, the processing extension must be registered in the CMC.

Processing extensions do not apply to Web Intelligence documents, Crystal reports in `.rptr` format, or reports created in SAP Crystal Reports for Enterprise.

1. Go to the *Folders* management area of the CMC.
2. Select the report object to apply a processing extension to.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Extensions* in the navigation list.
5. In the *Available processing extensions* list, select a processing extension, and click to move it to the *Use these processing extensions (in the order listed)* list.

   The *Available processing extensions* list contains only registered processing extensions.
6. Use the *Move Up* and *Move Down* buttons to set the order in which to use processing extensions.
7. Click *Save & Close*.

The processing extension(s) are assigned to the report object.

17.11 Showing a thumbnail image of a Crystal report's first page

1. Go to the *Folders* management area of the CMC.
2. Locate and select the report for which to show a thumbnail image of the first page.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Thumbnail* in the navigation list.
5. Select the *Show report thumbnail* check box.
6. Click *Save & Close*.

17.12 Adding reports to the BI repository and adding hyperlinks

To avoid breaking hyperlinks between reports, add the reports first and then create hyperlinks.

This feature does not apply to Web Intelligence documents or to reports created in Crystal Reports for Enterprise. For more information about tasks in SAP Crystal Reports, see the SAP Crystal Reports Help.

1. In Crystal Reports, create the reports without hyperlinks.
2. Add the reports to the BI platform repository.
3. Use Crystal Reports to log on to the platform.
4. Create hyperlinks between the home report and the destination report.

Crystal Reports automatically determines whether to establish a relative or absolute link between the reports. In the platform, relative links are assigned to reports in the same object package, and absolute links are assigned to individual report objects or instances.

17.13 Viewing the universes for a Web Intelligence document

In the CMC, you can view which universes are used by a Web Intelligence document.

A universe is a representation of the information available in a database. You build queries for Web Intelligence documents using objects in a universe.

1. Go to the *Folders* management area of the CMC.
2. Select the Web Intelligence document object for which to view universes.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Report Universes* in the navigation list.

A list of the universes used by the document appears.

17.14 Viewing Alerts in a Crystal report

You can view alerts for a Crystal report in the Central Management Console (CMC).

1. Go to the *Folders* management area of the CMC.
2. Locate the folder or category that contains the Crystal report to view, and select the report.
3. Select *More Actions* > *Alerts*.

   The *Alerts* dialog box appears, displaying the instances that triggered the alert.
4. Double-click an instance title to open an instance.

18 Program Objects

18.1 Specifying command-line arguments

For each program object, you can specify command-line arguments with the *Default Settings* command on the *Manage* menu.

You can specify any argument that is supported by the command-line interface for your program. Arguments are passed directly to the command-line interface, without parsing.

1. In the *Folders* management area of the CMC, select the program object.
2. Select *Manage* > *Default Settings*.
3. In the *Default Settings* dialog box, click *Program Parameters* on the navigation list.
4. In the *Arguments* box, enter the command-line arguments for your program, using the same format as at the command line.

   For example, if your program has a loops option, to set the loops value to 100, you might type `-loops 100`
5. Click *Save & Close*.

18.2 Setting the working directory for a program object

1. In the *Folders* management area of the CMC, select the program object.
2. Select *Manage* > *Default Settings*.
3. In the *Default Settings* dialog box, click *Program Parameters* on the navigation list.
4. In the *Working Directory* box, enter the full path to the directory that you want to set as the program object's working directory.

   For example, on Windows, if you created a working directory named `working_directory`, enter `C:\working_directory`. On Unix, enter `/working_directory`.
5. Click *Save & Close*.

18.3 Modifying the default working directory for a program object

1. Go to the *Servers* management area of the CMC.
2. Select the Adaptive Job Server that hosts the Program Scheduling Service.

   To check whether an Adaptive Job Server hosts the Program Scheduling Service, select the server and select *Manage* > *Properties*.

3. Select *Manage* > *Properties*.
4. In the *Properties* dialog box, in the *Temporary Directory* box, enter the full path to the directory to set as the working directory.
5. Click *Save & Close*.

18.4 Specifying the path to external or auxiliary files

You must specify the location of external or auxiliary files to some binary files, batch files, and shell scripts.

1. Go to the *Folders* management area of the CMC.
2. Select the executable program object for which to specify the path.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Program Parameters*.
5. In the *External Dependencies* box, enter the full path to the file, and click *Add*.
6. To edit or remove external dependencies, select the path under *External Dependencies*, and click *Edit* or *Remove*.
7. Repeat step 5 for each external or auxiliary file for which to specify the path.
8. Click *Save & Close*.

18.5 Uploading external or auxiliary files to the File Repository Server

1. Go to the *Folders* management area of the CMC.
2. Select the executable program object for which to upload files.
3. Select *Actions* > *Associated Files*.
4. Click *Browse* and locate the required file, and click *Add File*.
5. Repeat step 4 for each file to upload.
6. Click *Save & Close*.

18.6 Adding an environment variable

In the CMC, you can configure an executable program object by adding or modifying environment variables.

Modifications to an existing environment variable override the default variable (that is, changes are not appended to it). However, the changes you make to environment variables exist only in the temporary shell in which Information platform services runs the program. Thus, when the program exits, the environment variables are destroyed.

For example, to set the path variable to append a user's `bin` directory to the existing path:

- On Windows, enter: **`path=%path%;c:\usr\bin`**
- On Unix, enter: **`PATH=$PATH:/usr/bin`**

1. Go to the *Folders* management area of the CMC.
2. Select the executable program object for which to add an environment variable.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Program Parameters*.
5. In the *Environment Variables* box, enter the environment variable as **`<name>=<value>`**, and click *Add*.

   `<name>` is the environment variable name, and `<value>` is the value for the environment variable. Information platform services sets your environment variables using the syntax that is appropriate for your operating system. However, on Unix, you must follow convention and use the appropriate case. For example, all name values on Unix must be in uppercase.
6. Click *Save & Close*.

18.7 Specifying required parameters for Java programs

To successfully schedule and run a Java program, you must provide Information platform services with the base name of the `.class` file that implements the IProgramBase interface from the SAP BusinessObjects Enterprise Java SDK.

The Java Runtime Environment must be installed on each machine that is running an Adaptive Job Server.

1. Go to the *Folders* management area of the CMC.
2. Select the Java program object for which to specify required parameters.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Program Parameters* in the navigation list.
5. In the *Class to run* box, enter the base name of the `.class` file that implements the `IProgramBase` from the SAP BusinessObjects Enterprise Java SDK (`com.businessobjects.sdk.plugin.desktop.program.IProgramBase`). For example, if the file name is `Arius.class`, enter **`Arius`**.
6. Click *Save & Close*.

18.8 Providing Java programs with access to other files

You can provide Java programs with access to files, such as Java libraries, on the Program Scheduling Service machine.

The Java Runtime Environment must be installed on each machine that is running an Adaptive Job Server.

1. Go to the *Folders* management area of the CMC.
2. Select the Java program object for which to provide access to files on the Adaptive Job Server that hosts the Program Scheduling Service.

3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Program Parameters* on the navigation list.
5. In the *Classpath* box, enter the full path to each required Java library file that is stored on the Adaptive Job Server hosting the Program Scheduling Service.

   Separate paths with the classpath separator for your operating system. For example, use a semicolon to separate paths in Windows, and use a colon to separate paths in Unix.
6. Click *Save & Close*.

18.9 Specifying a user account for a program object

The Java Runtime Environment must be installed on each machine that is running an Adaptive Job Server.

1. Go to the *Folders* management area of the CMC.
2. Select the executable program object for which to specify a user account.
3. Select *Manage* > *Default Settings*.
4. In the *Default Settings* dialog box, click *Program Logon* on the navigation list.
5. In the *User Name* box and the *Password* box, enter the credentials for the user account under which the program should run.
6. Click *Save & Close*.

19 Object Packages

19.1 To create a new object package

1. Go to the *Folders* management area of the CMC and navigate to the folder that you want to create the object package in.
2. Click *Manage* > *New* > *Object Package*.
   The *Object Package* dialog box appears.
3. Enter a title, description, and keywords for your object package.
4. Click *OK*.

When the object package has been added to the system, you can modify the properties, contents, scheduling information, destination, user rights, object settings, and notification for the object package. To do this, use *Manage* > *Properties* or *Manage* > *Default Settings*.

19.2 To add a new object to an object package

1. In the *Folders* management area of the CMC, double-click an object package.
   The object package's contents are displayed in the *Details* panel.
2. Click *Manage* > *Add* > *Local Document* or *Program File* depending on the object you want to add.
   Different dialog boxes appear depending on the option you selected.
3. Click *Browse* and select the object that you want to add.
4. Set the appropriate properties.
   If you are adding a program object, set the program type by clicking *Executable*, *Java*, or *Script*.
5. Click *OK*.

19.3 To set component failure options for an object package

Perform this task to specify how component failure affects an object package at run time.

1. In the *Folders* management area of the CMC, navigate to the object package and select it.
2. Click *Manage* > *Default Settings*.
3. Click *Component Failure* on the navigation list.
4. Select or deselect the *Scheduled package fails upon individual component failure* check box.
5. Click *Save & Close*.

20 Scheduling

20.1 Scheduling an object

To quickly change the default schedule settings for an object, click *Default Settings* in the *Schedule* dialog box, set the scheduling options, and click *Save*.

1. Go to the *Folders* management area of the CMC.
2. Select the object to schedule.
3. Select *Actions* > *Schedule* .
   The *Schedule* dialog box appears, showing the default settings for the object.
4. Enter a title for the instance.
5. Click *Recurrence*, and select a recurrence pattern.
   For example, select *Weekly* to run the object one time per week.
6. Specify run options and scheduling parameters.

   > **Note**
   >
   > The option *Generate separate CSV per Data Provider* is currently available only for *FTP* and *File System* destinations.

   For example, select *Monday*, *Wednesday*, and *Friday*.
7. Click *Schedule*.

The BI platform creates a scheduled instance and runs it according to the schedule you specified. You can view scheduled instance in the *History* dialog box for the object.

> **Note**
>
> You can also schedule a report to multiple destinations in one go while scheduling the BI content in the Central Management Console (CMC) or the BI Launch pad. When you use the CMC, the values you select become the default scheduling values in the launch pad.
>
> For more information on scheduling destination options, refer to Scheduling destination options [page 394].

Related Information

Recurrence patterns [page 254]
Run Options for Recurrence Patterns [page 255]

20.1.1 Recurrence patterns

First select a recurrence pattern and then select run options for the recurrence pattern.

Recurrence pattern	Description
Now	The object runs when a user clicks *Schedule*.
Once	The object runs once. You specify at which time it will run and the start and end dates.
Hourly	The object runs hourly. You specify how often the object runs, at which time it will run, and the start and end dates.
Daily	The object runs once every <N> days. You specify how often the object runs, at which time it will run, and the start and end dates.
Weekly	The object runs every week. You specify on which days and at which time it will run and a start and end date.
Monthly	The object runs every <N> months. You specify how often the object runs, at which time it will run, and the start and end dates.
Nth Day of Month	The object runs on the <N> day of every month. You specify the day of the month, at which time it will run, and a start and end date.
1st Monday of Month	The object runs on the first Monday of every month. You specify at which time it will run and a start and end date.
Last Day of Month	The object runs on the last day of every month. You specify a start and end date.
X Day of Nth Week of the Month	The object runs on a particular day of a particular week each month. You specify the week and day it will run, at which time it will run, and the start and end date.
Calendar	The object runs on the dates specified in a calendar.
Business Hours	The object runs on the particular days of the week and during the particular hours of the day that are specified under business days and *Business Hours*.

Related Information

Run Options for Recurrence Patterns [page 255]

20.1.2 Run Options for Recurrence Patterns

First select a recurrence pattern and select run options for the pattern. Not all run options are available for all objects. When you select a run option that contains a variable, the BI platform displays the variable's default value. You can change default values as needed.

Run option for recurrence patterns	Description
Start Date/Time	These lists appear for all recurrence patterns, except *Now* and *Calendar*. Select the time (hours, minutes, and A.M. or P.M.) and the date on which to start running the object. The platform runs the object according to the specified schedule, as soon as it can after the start time has passed. The default is the current date and time. For example, if you specify a start time that is three months in the future, the platform waits to run the object until the start date has passed, even if all other criteria are met. After the start date, the platform runs the report at the specified time.
End Date/Time	These lists appear for all recurrence patterns, except *Now* and *Calendar*. Select the time (hours, minutes, and AM or PM) and the date on which to stop running the object. After the end time has passed, the platform no longer runs an object. The default is the current time and a date in the distant future, to ensure an object will run indefinitely.
Hour(N) and *Minute(X)*	These lists appear when you select the *Hourly* recurrence pattern. Select the interval (in hours and minutes) at which to run the object. If you do not enter a value for `<N>` or `<X>`, the platform runs the report every hour.
Days(N)	This box appears when you select the *Daily* recurrence pattern. Enter the interval (in days) at which to run the object. If you do not enter a value for `<N>`, the platform runs the report every day
Monday, *Tuesday*, *Wednesday*, *Thursday*, *Friday*, *Saturday*, and *Sunday*	These check boxes appear when you select the *Weekly* and *Business Hours* recurrence pattern. Select the check box beside each day of the week on which to run the job.

Run option for recurrence patterns	Description
Month(N)	This list appears when you select the *Monthly* recurrence pattern. Enter the interval (in months) at which to run the object. If you do not enter a value for `<N>`, the platform runs the report every month.
Day(N)	This box appears when you select the *Nth Day of Month* recurrence pattern. Select the day of the month on which to run the object. If you do not select a value for `<N>`, the platform runs the report every day.
Week(N) and *Day(X)*	These lists appear when you select the *X Day of Nth Week of the Month* recurrence pattern. Select the week in the month and the day of the week on which to run the object. If you do not enter a value for `<N>` or `<X>`, the platform runs the report every day.
Business Hours Start	This box appears when you select the *Business Hours* recurrence pattern. Enter the start time of your business or working day.
Business Hours End	This box appears when you select the *Business Hours* recurrence pattern. Enter the end time of your business or working day.

20.2 Scheduling an object to Default Enterprise Location

To save instances only to the Output File Repository Server (FRS)—not to any other destination—use the *Default Enterprise Location* destination.

1. Go to the *Folders* management area of the CMC.
2. Select the object for which to set the default destination.
3. Select *Actions* > *Schedule* >.
4. Click *Destinations*.
5. In the *Destination* list, select *Default Enterprise Location*.
6. Click *Schedule*.

20.3 Scheduling an object to a file location

When scheduling objects, you can configure objects for output to an unmanaged disk. In this case, the BI platform saves an output instance to the Output File Repository Server (FRS) and to the specified destination.

Before scheduling an object to a file location:

- The file location must be a local directory on the processing server. For servers on Windows, the location can be a Universal Naming Convention (UNC) path or a local directory.
- The file location must be enabled and configured on the Adaptive Job Server.
- The processing server must have sufficient access rights to the file location.

If the object is a Web Intelligence document or an object package, you cannot choose an unmanaged disk as a destination. However, for an object package, you can configure individual objects in the object package for output to an unmanaged disk.

1. Go to the *Folders* management area of the CMC.
2. Select an object to schedule.
3. Select *Actions* > *Schedule* >.
4. Click *Destinations*.
5. In the *Destination* list, select *File System*.
6. Select or clear the *Keep an instance in the history* check box.
7. Select or clear the *Use default settings* check box.

   If you selected the *Use default settings* check box, go to step 9.
8. If you cleared the *Use default settings* check box, perform the following actions:
   a. In the *User Name* box, enter a user name with access rights to save files to the destination directory.
   b. In the *Password* box, enter the user password that is required to access the destination directory.
   c. In the *Directory* box, enter a local hard disk location, mapped location, or UNC path to the directory where you want to send the instance.
   d. Under *File Name*, select *Use Automatically Generated Name* or *Use Specific Name*.
9. Click *Schedule*.

20.4 Scheduling an object to an FTP server

When scheduling objects, you can configure the objects for output to a File Transfer Protocol (FTP) server. To connect to the FTP server, you must specify a user who has the necessary rights to upload files to the server. If you specify an FTP destination, the system will save an output instance to both the Output File Repository Server and the specified destination.

Before you can use this destination, it must be enabled and configured on the Adaptive Job Servers.

1. Go to the *Folders* management area of the CMC.
2. Select an object to schedule.
3. Select *Actions* > *Schedule* >.

4. Click *Destinations*.
5. In the *Destination* list, select *FTP Server*.
6. Select or clear the *Keep an instance in the history* check box.
7. Select or clear the *Use default settings* check box.

   If you selected the check box, go to step 9.
8. If you cleared the *Use default settings* check box, perform the following actions:
   a. In the *Host* box, enter the IP address of the FTP server host computer to send the instance to.
   b. In the *Port* box, enter the port of the FTP server to send the instance to.
   c. In the *User Name* box, enter a user name with access rights to upload the object to the FTP server.
   d. In the *Password* box, enter the user password that is required to access the FTP server.
   e. In the *Account* box, enter the account that is required to access the FTP server.
   f. In the *Directory* box, enter the path to the FTP directory where you want to send the instance.
   g. Under *File Name*, select *Use Automatically Generated Name* or *Use Specific Name*.
9. Click *Schedule*.

20.5 Scheduling an object to an SFTP server

When scheduling objects, you can configure the objects for output to a Secure File Transfer Protocol (SFTP) server. To connect to the SFTP server, you must specify a user who has the necessary rights to upload files to the server. If you specify an SFTP destination, the system will save an output instance to both the Output File Repository Server and the specified destination.

Before you can use this destination, it must be enabled and configured on the Adaptive Job Servers.

1. Go to the *Folders* management area of the CMC.
2. Select an object to schedule.
3. Select *Actions* > *Schedule* >.
4. Click *Destinations*.
5. In the *Destination* list, select *SFTP Server*.
6. Select or clear the *Keep an instance in the history* check box.
7. Select or clear the *Use default settings* check box.

   If you selected the check box, go to step 9.
8. If you cleared the *Use default settings* check box, perform the following actions:
   a. In the *Host* box, enter the IP address of the SFTP server host computer to send the instance to.
   b. In the *Port* box, enter the port of the SFTP server to send the instance to.
   c. In the *User Name* box, enter a user name with access rights to upload the object to the SFTP server.
   d. In the *Password* box, enter the user password that is required to access the SFTP server.
   e. In the *Account* box, enter the account that is required to access the SFTP server.
   f. In the *Directory* box, enter the path to the SFTP directory where you want to send the instance.
   g. Under *File Name*, select *Use Automatically Generated Name* or *Use Specific Name*.
   h. In the *Fingerprint* box, enter the host key fingerprint of the SFTP server.
9. Click *Schedule*.

20.6 Scheduling an object to email

When you select the *Email* destination, the BI platform saves the output instance to the Output File Repository Server and sends a copy of the instance as an attachment to the email addresses you specify.

Before you can use this destination, the *Email* (SMTP) destination must be enabled and configured on the Adaptive Job Servers.

Crystal report and other object instances are sent to email destinations via Simple Mail Transfer Protocol (SMTP) mail support.

The BI platform supports Multipurpose Internet Mail Extensions (MIME) encoding.

1. In the CMC, select the *Folders* area.
2. Select an object to schedule.
3. Select *Actions* > *Schedule* >.
4. Click *Destinations*.
5. In the *Destination* list, select *Email*.
6. Select or clear the *Keep an instance in the history* check box.
7. Select or clear the *Use default settings* check box.

   If you selected the *Use default settings* check box, go to step 9.
8. If you cleared the *Use default settings* check box, perform the following actions:
   a. In the *From* box, enter the return email address.
   b. In the *To* box, enter the email address of each recipient to send the instance to.
   c. In the *Cc* box, enter the email address of each recipient to send a copy of the email and instance to.
   d. In the *Bcc* box, enter the email address of each undisclosed recipient to send a copy of the email and instance to.
   e. In the *Subject* box, enter the subject of the email.
   f. In the *Message* box, enter a message for the body of the email.
   g. Select or clear the *Add Attachment* check box.
   h. Under *File Name*, select *Use Automatically Generated Name* or *Use Specific Name*.
9. Click *Schedule*.

Related Information

Enabling or disabling destinations for a job server [page 261]

Setting up SMTP over SSL

To setup SMTP over SSL, it is required that the same certificate be present in the Server and the Client systems.

To setup SMTP over SSL, follow the below mentioned steps:

1. On the Windows platform, go to `<install_dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. In addition, for clients connected to the BI Platform, go to `<install_dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.`

   > **i Note**
   >
   > For all other supported platforms, navigate to the respective folders.

2. Name the certificate as "certificate.crt".

   For example, While connecting to the SMTP server, the server will send the certificate detail. The certificate detail needs to copied to a raw text file and renamed as “certificate.crt”. This must be placed in the win64_x64 folder for the windows platform. and in the win32_86 folder for the clients.

SMTP over SSL is now setup.

> **i Note**
>
> When the user checks the *Enable SSL* checkbox, a secure channel is enabled. This allows secure SMTP transmission over SSL.

20.7 Scheduling an object to user BI Inboxes

When scheduling objects, you can configure an object to send its instances to one or more user BI Inboxes. The BI platform stores the instance on the Output File Repository Server (FRS) and sends a copy of the instance to the BI Inboxes you specify.

By default, the BI Inbox destination is enabled and configured on the Adaptive Job Servers.

1. Go to the *Folders* management area of the CMC.
2. Select an object to schedule.
3. Select *Actions* > *Schedule* > .
4. Click *Destinations*.
5. In the *Destination* list, select *BI Inbox*.
6. Select or clear the *Keep an instance in the history* check box.
7. Select or clear the *Use default settings* check box.

   If you selected the *Use default settings* check box, go to step 9.
8. If you cleared the *Use default settings* check box, perform the following actions:
   a. Under *Available Recipients*, select users to send the instance to.
   b. Under *Target Name*, select *Use Automatically Generated Name* or *Use Specific Name*.
   c. Under *Send As*, select *Shortcut* or *Copy*.
9. Click *Schedule*.

20.8 Enabling or disabling destinations for a job server

By default, when the BI platform runs a scheduled report or program object, it stores the output instance it creates on the Output File Repository Server (FRS). When you choose a destination (other than Default Enterprise Location) to schedule or send an object to, the BI platform stores the output instance on the Output FRS and saves a copy at the destination you specify.

Before choosing a destination, the destination must be enabled and configured on the Adaptive Job Servers.

By default, the BI Inbox destination is enabled and configured on the Adaptive Job Servers so that you can distribute reports and documents. You can enable and configure additional destinations on the Adaptive Job Server.

1. Go to the *Servers* management area of the CMC.
2. Select the Adaptive Job Server for which to enable or disable a destination.
3. Select *Manage* > *Properties*.
4. In the *Properties* dialog box, click *Destinations*.
5. Perform one of the following actions:
   - To enable a destination, select it in the *Destination* list, click *Add*, and configure it.
   - To disable a destination, select it in the *Destination* list, and click *Remove*.
6. Click *Save* or *Save & Close*.

20.9 Scheduling an object based on an event

Perform this task to run a scheduled job after an event has occurred.

1. Go to the *Folders* management area of the CMC.
2. Select the object to run based on an event.
3. Select *Actions* > *Schedule*.
4. Click *Recurrence* in the navigation list.
5. In the *Run object* list, select a run option.
6. Set the remaining recurrence options for the object (start date, end date, and so on) as needed.
7. Click *Events* in the navigation list.
8. Under *Available Events*, select one or more events, and click to add the event(s) to the *Events to wait for* list.
9. Click *Schedule*.

Related Information

Recurrence patterns [page 254]

Run Options for Recurrence Patterns [page 255]
Events and Scheduling [page 276]

20.10 Scheduling an object to trigger an event

Perform this task to trigger an event when a scheduled job runs.

1. Go to the *Folders* management area of the CMC.
2. Select the object that should trigger the event.
3. Select *Actions* > *Schedule* > .
4. Click *Recurrence* in the navigation list.
5. In the *Run object* list, select a run option.
6. Set the remaining recurrence options for the object (start date, end date, and so on) as needed.
7. Click *Events* in the navigation list.
8. Under *Available Schedule Events*, select one or more events, and click to add the event(s) to the *Events to trigger on completion* list.

   You can select only schedule-based events.
9. Click *Schedule*.

Related Information

Recurrence patterns [page 254]
Run Options for Recurrence Patterns [page 255]

20.11 Configuring success or failure notification for an instance

If a notification option is available but not selected, it is labeled "Not in use." If a notification type is in use, it is labeled "Enabled."

1. Go to the *Folders* management area of the CMC.
2. Select an object for which to set notification.
3. Select *Actions* > *Schedule* > .
4. On the navigation list, click *Notification*.
5. To use audit notification, click *Audit Notification*, and perform the following actions:
   - To send a record to the auditing database when a job succeeds, select the *A job has been run successfully* check box.

- To send a record to the auditing database when a job fails, select the *A job has failed to run* check box.

6. To use email notification, click *Email Notification*, and perform the following actions:
   - To send an email when a job succeeds, select the *A job has been run successfully* check box.
     To specify the content and recipients of the email, select *Set the values to be used here*, and enter email addresses in the *From* and *To* boxes, enter a subject, and enter the message. Separate multiple addresses or distribution lists with semicolons.
   - To send an email when a job fails, select the *A job has failed to run* check box.
     To specify the content and recipients of the email, select *Set the values to be used here*, and enter email addresses in the *From* and *To* boxes, enter a subject, and enter the subject, and enter the message. Separate multiple addresses or distribution lists with semicolons.

   By default, the notification is sent to the server's default email destination.

20.12 Setting an alert notification

1. Go to the *Folders* management area of the CMC.
2. Select a report object for which to set alerts.
3. Select *Actions* > *Schedule* > .
4. In the *Schedule* window, click *Notification*.
5. Select the *Enable alert notification* check box.
6. Select *Use default settings* to deliver alert notification using the default Adaptive Job Server settings, or select *Custom settings* and specify the email settings.

   You can change the default Adaptive Job Server settings in the *Servers* area of the CMC. For more information, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
7. Enter the URL of the viewer that you want recipients to use for the report, or select the default viewer.

   You must use World Wide Web Consortium (W3C) encoding for the viewer URL. For example, replace spaces in the path with **%20**. For more information, see http://www.w3.org/ .

   To set a viewer URL as the default, select *Central Management Console* in the *Applications* area of the CMC, select *Actions* > *Processing Settings* > , and enter the URL in the *URL (must be URL encoded)* box.

   The viewer URL will appear as a hyperlink in the alert notification email.
8. Enter the maximum number of alert records to include in an alert notification.

   A hyperlink in the alert notification will go to a report page containing the records that triggered the alert.

   You enter the alert name and status in SAP Crystal Reports.
9. Click *Schedule*.

20.13 Selecting an output file format

1. Go to the *Folders* management area of the CMC.

2. Select a report object for which to choose an output file format.
3. Select *Actions* > *Schedule* >.
4. Click *Formats*.
5. Select an output format.
   For example, for a Crystal report, select a format under *Format Options for Selected Document*, and for a Web Intelligence document, select a format under *Output Format*.
6. Set the remaining scheduling options as needed.
7. Click *Schedule*.

20.14 Selecting a cache format for Web Intelligence documents

When the BI platform runs a scheduled Web Intelligence document, it stores the generated instance on the Output File Repository Server (FRS). When you select a cache format, the platform caches the instance on the appropriate report server. If you do not select a cache format, the system cannot cache the instance.

Selecting a cache format applies only to Web Intelligence documents, not to Crystal reports.

1. Go to the *Folders* management area of the CMC.
2. Select a Web Intelligence document object for which to select a cache format.
3. Select *Actions* > *Schedule* >.
4. Click *Caching*.
5. Under *Available Formats to Cache*, select *Microsoft Excel*, *Standard HTML*, and/or *Adobe Acrobat*.

   You can select more than one format.

   The cache is preloaded with the format(s) you selected.
6. Under *Available locales*, select the locale(s) to preload the cache with, and click to move the locale(s) to the *Selected locales* list.

   You can select more than one locale. When you schedule this Web Intelligence document, the platform generates cached versions of the document in these locale(s).

   The cache is preloaded with the locale(s) you selected.
7. Set the remaining scheduling options as needed.
8. Click *Schedule*.

20.15 Scheduling a report object for individual users

1. Go to the *Folders* management area of the CMC.
2. Select a report object to schedule.
3. Select *Actions* > *Schedule* >.

4. Click *Schedule For*.
5. Select *Schedule only for myself* or *Schedule for specified users and user groups*.
6. If you selected *Schedule for specified users and user groups*, locate and select the users or user groups for which to generate a report instance, and click > to add them to the *Selected* list.

   To remove a user or group from the *Selected* list, select the user or group, and click <.
7. Specify the remaining scheduling options, and click *Schedule*.

Related Information

Recurrence patterns [page 254]
Run Options for Recurrence Patterns [page 255]

20.16 Selecting a server or server group for a scheduled object

You can choose the server or server group on which a scheduled object will run, which gives you more control over load balancing.

You can choose the server group that the BI platform uses when a user refreshes a Crystal report or Web Intelligence document instance while viewing it. In addition, you can run program jobs on a specific server group so they do not monopolize system resources.

The options in this task are available when you select *Manage* > *Default Settings*, and *Viewing Server Group* (Crystal reports) or *Web Intelligence Process Settings* (Web Intelligence documents).

1. Go to the *Folders* management area of the CMC.
2. Select the object to schedule.
3. Select *Actions* > *Schedule*.
4. Click *Scheduling Server Group* in the navigation list.
5. Choose the type of server to use:
   - Select *Use the first available server* to run the object as quickly as possible, regardless of the server group used.
   - Select *Give preference to servers belonging to selected group* to use a specific server in a server group, if more than one server is available.
   - Select *Only use servers belonging to the selected group* to use the specified server group, and enter the server group.

   If you are scheduling a program object that requires access to files stored locally on the Adaptive Job Server that hosts the Program Scheduling Service, but you have multiple Adaptive Job Servers, you must specify which server to use to run the program.
6. Select the *Run at origin site* check box to run the object at the site where it is located.
7. Set the remaining scheduling options as required, and click *Schedule*.

20.17 Managing instances for an object

Perform this task to view and manage instances for a specific object. To view and manage instances for all objects, use the Instance Manager instead.

1. Go to the *Folders* management area of CMC.
2. Select the object for which to manage instances.
3. Select *Actions* > *History*.
4. Select an instance or instances.

   To refresh the list, click *Refresh*. In this case, you do not need to select an instance first.
5. Select *Run Now*, *Pause*, *Resume*, *Send to*, *Reschedule*, or *Delete*.

   If you select *Run Now*, the BI platform schedules the object to run immediately. The scheduled job has a status of Pending.

Related Information

Instance Manager [page 266]

20.18 Instance Manager

Use the Instance Manager to view and to manage all instances in your BI platform deployment from one location.

You can use the Instance Manager to perform the following tasks:

- Find specific instances
- Select multiple instances and perform batch operations on them (for example, pause, resume, or delete)
- View detailed information for a single instance
- Diagnose and resolve system problems that cause instances to fail

The default view of the Instance Manager shows all pending instances, sorted by title. To view detailed information about an instance, select the instance and click the *Instance details* icon on the toolbar.

Example: Using the Instance Manager for troubleshooting

An administrator logs on to the CMC, checks the Instance Manager, and notices that several jobs have failed. The administrator filters the list to show only failed jobs from the last two days, and notices that they all seem to have run on the same server. The administrator sorts the list by server and verifies that all failed jobs ran on the same server. The error code for each failure is the same. The administrator views detailed information for an instance and discovers that a database connection has been reconfigured improperly. The administrator

reconfigures the database connection correctly and returns to the Instance Manager to rerun all of the failed jobs.

20.19 Viewing an instance

You can also use the Instance Manager to view a list of instances by status or by user.

1. Go to the *Folders* management area of CMC.
2. Select the object for which to view an instance.
3. Select *Actions* > *History*.
4. In the *Instance Time* column, click the instance to view.

Scroll to the right in order to view all columns in the default width. You cannot sort instances using the submission time, start time, duration, recurrence, or expiry columns.

Related Information

Instance Manager [page 266]

20.20 Pausing an instance

1. Open the *History* dialog box for an object.
2. Select the scheduled instance to pause, and click *Pause*.

20.21 Resuming a paused instance

1. Open the *History* dialog box for an object.
2. Select the scheduled instance to resume, and click *Resume*.

20.22 Deleting an instance

You can delete instances from an object as needed. You can delete both scheduled instances, which have a status of recurring or pending, and report or program instances, which have a status of success of failed.

1. Open the *History* dialog box for an object.
2. Select the instance(s) to delete, and click *Delete*.

20.23 Setting limits for instances

You set limits, at the object or folder level, to automate the regular cleanup of old instances.

At the object level, you can limit the number of instances that remain in the BI platform for an object, user, or user group, or limit the number of days that an instance remains in the platform for a user or group. When you set limits at the object level, the limits override any limits set for folders. (That is, the object does not inherit the limits of the folder.)

At the folder level, when you set limits, the limits affect all objects in the folder, including its subfolders.

1. Go to the *Folders* management area of CMC, and select an object.
2. Select *Actions* > *Limits*.
3. In the *Limits* dialog box, perform one of the following actions:
   - To limit the number of instances per object, select the *Delete excess instances when there are more than N instances of an object* check box, and enter the maximum number of instances that should remain on the system.
     The default value is 100.
   - To limit the number of instances for users or groups, select the *Delete excess instances for the following users/groups* check box, click *Add*, select users or groups and click > to move them to the list, click *OK*, and enter the maximum number of instances in the *Instance Limit* column.
     The default value is 100.
   - To limit the number of days that instances are saved for users or groups, select the *Delete instances after N days for the following users/groups* check box, click *Add*, select users or groups and click > to move them to the list, click *OK*, and enter the maximum age of instances in the *Maximum Days* column.
     The default value is 100.
4. Click *Update*.

Related Information

Limiting report instances at the folder level [page 229]

20.24 Running multiple objects now

Instead of scheduling individual objects, you can run multiple objects from the CMC using *Run Now*. When you run objects now, they are run instantly using their default scheduling settings.

1. Go to the *Folders* management area of the CMC.
2. Locate and select the object(s) to run.
3. Select *Actions* > *Run Now*.

20.25 To select languages for report instances

> **Note**
>
> This task applies to SAP Crystal Reports only.

Perform this task if you want to generate report instances in different languages.

1. In the *Schedule* dialog box, click *Languages*.
2. Select a language option.
   - *Schedule the report in Preferred Viewing Locale*
     This option schedules the report according to the preferred viewing locale you set in your preferences, and creates instances using that locale only.
   - *Schedule the report in Multiple Locales*
     This options schedules the report in multiple languages. If you choose this option, you must also select locales by moving them from the *All Locales* list to the *Selected Instance Locales* list.
3. Set other scheduling parameters as required, and click *Schedule*.

21 Calendars

21.1 Creating a calendar

It is good practice to create a calendar for users to use as a template for creating new calendars. They can copy this template calendar and modify it as necessary. For example, you can create a default Weekdays calendar that includes all days as run dates except weekends and company holidays.

1. Go to the *Calendars* management area of the CMC.
2. Select *Manage* > *New* > *New Calendar*.
3. Enter a name and description for the calendar, and click *OK*

The calendar is added to the system, and you can add run dates to it on the *Dates* tab.

Related Information

Adding dates to a calendar [page 270]

21.2 Adding dates to a calendar

After creating a calendar, you can view dates in a yearly, quarterly, or monthly format before adding them to the calendar, and you can choose recurring dates based on the day of month or week.

When changing an existing calendar, the BI platform checks all currently scheduled instances on your system, and updates the objects that use the calendar. These are automatically updated to run on the revised date schedule.

1. Go to the *Calendars* management area of CMC.
2. Select the calendar to which to add dates.
3. Select *Actions* > *Select Dates*.
4. Select the *Yearly*, *Quarterly*, or *Monthly* calendar format.
5. To create a calendar with recurring dates, select *By day of month* or *By day of week*.
6. Select the days of the month when the calendar should run.

   To remove a run day, click the day. To select a week or all weekdays in a month as run days, click the row or column header.
7. When you are finished, click *Save*.

21.3 Deleting a calendar

When a calendar is deleted, the BI platform will run objects scheduled by the deleted calendar one more time.

Before deleting a calendar, check the scheduling information for objects to which the calendar was applied. You will want to ensure that required objects continue to run. If necessary, you can select a different calendar or a different recurrence pattern for the objects.

1. Go to the *Calendars* management area of the CMC.
2. Select the calendar to delete.
   To select multiple calendars, hold down the CTRL or SHIFT key and click each calendar.
3. Select *Manage* > *Delete*, and click *OK*.

Related Information

Scheduling an object [page 253]

22 Events

22.1 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.

22.1.1 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.

22.1.1.1 Creating a Notification Event

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:

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*.

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.

22.1.1.2 Selecting a Notification Audience

Notification capability allows you to select the required audience for every notification you create.

To select the audience for a notification, proceed as follows:

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*.

You have now successfully selected the audience for a notification.

> **i Note**
>
> You cannot modify the subscription list after the notification is triggered.

22.1.1.3 Editing a Notification Event

To edit a notification event, proceed as follows:

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.

   > **i 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*.

You have now successfully edited a notification event.

> **i 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.

22.2 Events and Scheduling

Events are objects that represent occurrences in the system.

Depending on the event type, they can be used for scheduling, alerting, or monitoring system health. The *Events* management area of CMC organizes all events into folders according to event type. Within each event type folder, you can create subfolders to better store and manage events.

Event-based scheduling provides you with additional control over scheduling objects: you can set up events so that objects are processed only after a specified event occurs. Working with events consists of two steps: creating an event and scheduling an object with events. That is, once you create an event, you can select it as a dependency when you schedule an object. The scheduled job is then processed only when the event occurs.

You can create the following types of events to be used in conjunction with scheduling:

Type of event	Description
File events	When you define a file-based event, you specify a file name that the *Event Server* monitors for a particular file. When the file appears, the *Event Server* triggers the event. For instance, you might want to make some reports dependent upon the regular file output of other programs or scripts. File events are stored in the *System Events* folder.
Schedule events	When you define a schedule-based event, you select an object whose existing recurrence schedule will serve as the trigger for your event. In this way, schedule-based events allow you to set up contingencies or conditions between scheduled objects. For instance, you might want certain large reports to run sequentially, or you might want a particular sales summary report to run only when a detailed sales report runs successfully. Schedule events are stored in the *System Events* folder.

Type of event	Description
Custom events	When you create a custom event, you create a shortcut for triggering an event manually. Custom events are stored in the *Custom Events* folder.

When scheduling with events, keep in mind that an object's recurrence schedule determines how frequently the object runs. For instance, a daily report that is dependent upon a file-based event will run once a day (as long as the file that you specify appears every day). In addition, the event must occur within the time frame established when you actually schedule the event-based report.

Use file-based events for alerting.

Automatically created events

The system automatically creates corresponding events when certain types of objects (for example, Crystal reports) are added to the repository.

> **Note**
>
> You can view these types of events in the *Events* area. However, to manage or modify these types of events, you must have access to the corresponding event source or the relevant application.

Monitoring events

To monitor the overall health of the system, the BI platform offers Monitoring events. These events correspond to the Monitoring probes that are created and managed in the *Monitoring* area.

22.2.1 Creating a file-based event

File-based events are stored and managed in the *System Events* folder.

1. Go to the *Events* management area of CMC.
2. Locate and open the `System Events` folder.
3. Select *Manage* > *New* > *New Event*.
4. In the *Type* list, select *File*.
5. Enter a name for the event in the *Event Name* box.
6. Enter a description in the *Description* box.
7. In the *Server* list, select the event server that should monitor the specified file.
8. Enter a file name in the *Filename* box.

Enter the absolute path to the file that the event server should look for (for example, `C:\<folder>\<FileName>`, or `/home/<folder>/<FileName>`). The drive and directory that you specify must be visible to the event server. Ideally, the directory should be on a local drive.

9. To enable alerting for the event, select *Alerting Enabled*, and enter a message in the *Alert Message* box.
   When the event is triggered, this message will be included in the alert notification that is sent.
10. Click *OK*.

22.2.2 Creating a schedule-based event

Schedule-based events are stored and managed in *System Events*.

1. Go to the *Events* management area of CMC.
2. Locate and open the `System Events` folder.
3. Select *Manage* > *New* > *New Event*.
4. In the *New Event* dialog box, select *Schedule* in the *Type* list.
5. Enter an event name in the *Event Name* box.
6. Enter a description of the event in the *Description* box.
7. Select one of the following event status options:

Event status	Description
Success	The event is triggered only on successful completion of a specified object.
Failure	The event is triggered only on non-successful completion of a specified object.
Success or Failure	The event is triggered on completion of a specified object.

8. To enable alerting for the event, select *Alerting Enabled*.
   When the event is triggered, an alert notification will be sent to users.
9. Click *OK*.

22.2.3 Creating a custom event

First create a custom event, then schedule an object that depends on the event, and then trigger the event.

1. Go to the *Events* management area of the CMC.
2. Locate and open the `Custom Events` folder.
3. Select *Manage* > *New* > *New Event*.
4. Enter a name for the event in the *Event Name* box.
5. Enter a description of the event in the *Description* box.
6. To enable alerting for the event, select *Alerting Enabled*, and enter a message in the *Alert Message* box.
   When the event is triggered, this message will be included in the alert notification.

7. Click *OK*.

Related Information

Scheduling an object [page 253]
Enabling alerting for an event [page 280]

22.2.4 Triggering a custom event

1. Go to the *Events* management area of CMC.
2. Locate and open the `Custom Events` folder.
3. Select a custom event.
4. Select *Actions* > *Trigger Event*.

23 Alerting

23.1 Locating alert source objects in the CMC

Alert sources are stored in different locations according to their object type. The following table summarizes how to locate different alert sources.

Object (alert source)	Location in the CMC
Crystal reports	*Folders* or *Personal Folders* area A list of all Crystal report alerts in the system that support alerting is available in the `Crystal Reports Events` folder in the *Events* area of the CMC. To subscribe to an alert, locate the Crystal report in the *Folders* or *Personal Folders* area.
Events (file-based, schedule-based, and custom)	*Events* area Events are organized by event type. Alerting-enabled events are indicated by a icon.

23.2 Enabling alerting for an event

Alerting is automatically enabled for Crystal reports that contain alerts—that is, users can subscribe to report alerts as soon as a report is added to the repository.

Enabling alerting for events requires additional steps, such as enabling an alert when a new event is created.

1. Go to the *Events* management area of CMC.
2. Locate and select the event for which to enable alerting.
3. Select *Manage* > *Properties*.
4. In the *Properties* dialog box, click *Event Settings* in the navigation pane.
5. Select the *Alerting Enabled* check box, and enter a message in the *Alert Message* box to send to subscribers when the alert is triggered.

   You cannot enter messages for schedule-based events.
6. Click *Save & Close*.

23.3 Subscribing to an alert

1. Go to the *Events* management area of CMC.
2. Locate and select the alert source.
3. Select *Actions* > *Subscribe*.
4. In the *Subscribe to Publication* dialog box, under *Destinations*, select a destination for the alert:

Option	Description
My Alerts	Select this check box to send the alert notification to a destination in the Business Intelligence system (for example, BI launch pad).
Email	Select this check box to send the alert notification to the email address specified for your user account in the BI platform. This destination is available only if an email address was specified for your user account. Ensure that your email address is valid and entered correctly; otherwise, you will not receive the alert notification.

5. If multiple documents are listed under *Alert*, select the check box for each alert that you want to receive.
6. To specify a parameter for the alert, under *Parameters*, click *Edit*, and modify the parameter value.
   If a document is personalized, personalization details appear when you hover the mouse over an alert check box.
7. Configure the remaining alert subscription options as needed.
   Depending on the alert source, additional subscription options may appear. For example, for Crystal reports that contain multiple alerts, you must select which alert to subscribe to.
8. Click *OK*.

The next time the alert is triggered, a notification is sent to the destination you selected. To send the alert notification to a different destination, select the alert source, and select *Actions* > *Modify Subscription*. You can also use this option to select the Crystal report that an alert is subscribed to.

Notifications are sent using the destination defaults set for the alerting application, unless you specify custom settings for the alert source.

Related Information

Managing alerting settings for an alert source [page 283]
Locating alert source objects in the CMC [page 280]

23.4 Unsubscribing from an alert

1. Go to the *Events* management area of CMC.

2. Locate and select the alert source.
3. Select *Actions* > *Unsubscribe*.
4. In the *Unsubscribe from Alert(s)* dialog box, when prompted for confirmation, click *Unsubscribe*.

23.5 Subscribing other users to an alert

1. Go to the *Events* management area of CMC.
2. Locate and select the alert source.
3. Select *Actions* > *Manage Subscribers*.
4. In the *Manage Subscribers* dialog box, click *Subscriber List* in the navigation pane.
5. To add new subscribers:
   a. Click *Add*.
   b. In the *Add Subscribers* dialog box, use the > button to move users and groups from the *Available* list to the *Subscribed* list, and click *Add Default Subscription(s)*.
   c. In the *Edit Subscriptions* dialog box, configure the alert and destination options as needed.

      For example, you can modify which alerts to subscribe to (if the alert source contains multiple alerts). Depending on the alert source, other settings may be available.
   d. Click *Save & Close*.
6. To edit settings for a subscriber:
   a. Select a user in the *Subscriber* column, and click *Edit*.
   b. To edit which alerts the user will receive, in the *Edit Subscriptions* dialog box, click *Alerts* in the navigation list, and select the check box for each alert you want to subscribe the user to.

      If the alert source contains multiple alerts, each alert is listed. Otherwise, only one alert appears.
   c. To edit which destinations an alert will be sent to, click *Destinations* in the navigation list, and select the check box for each destination you want to sent the alert to.

      Only email destinations that are enabled and configured on the Adaptive Job Server are available. If no email destination is configured, only the *My Alerts* check box appears.
   d. If available, configure other alerting options as needed.

      Depending on the alert source, additional options may be available.
   e. Click *Save & Close*.
7. In the *Manage Subscribers* dialog box, click *Save & Close*.

23.6 Unsubscribing other users from an alert

1. Go to the *Events* management area of CMC.
2. Locate and select the alert source.
3. Select *Actions* > *Manage Subscribers*.

4. In the *Manage Subscribers* dialog box, click *Subscriber List* in the navigation pane.
5. Select a user or user group you want to stop subscribing alerts to, and click *Unsubscribe*.

23.7 Excluding users from an alert

Excluding users is useful when you want to subscribe only a handful of users in a group. You first subscribe the entire group and then exclude users who do not need to receive alert notifications.

The *Excluded* list overrides all other subscription settings for a user.

1. Go to the *Events* management area of CMC.
2. Locate and select the alert source.
3. Select *Actions* > *Manage Subscribers*.
4. In the *Manage Subscribers* dialog box, select *Excluded List* on the navigation panel.
5. Use the > button to move users or groups from the *Available* list to the *Excluded* list.
6. Click *Save & Close*.

Related Information

Locating alert source objects in the CMC [page 280]

23.8 Managing alerting settings for an alert source

Unless you change the alerting settings for an alert source, notifications are sent using the default destination settings for the Alerting application.

1. Go to the *Events* management area of CMC.
2. Locate and select the alert source.
3. Select *Actions* > *Manage Alerting Settings*.
4. In the *Manage Alerting Settings* dialog box, to enable the BI launch pad as a destination, select the *Enable My Alerts* check box.

   This option sends alert notifications to subscriber BI launch pad accounts, and subscribers can view them under *My Alerts* in the launch pad.
5. To enable email as a destination, select the *Enable Email* check box, and then select *Use default email settings* or *Use custom email settings*.

   If you selected *Use default email settings*, the default settings are derived from alerting values set in the *Applications* area.
6. If you selected *Use custom email settings*, perform the following actions as needed:

a. In the *From* box, enter a return email address, or select variables for the email address from the *Add placeholder* list.
b. In the *To* box, enter each email address that you want to send alert notifications to, or select variables for the email address from the *Add placeholder* list.
c. In the *Cc* box, enter each email address that you want to send alert notifications to, or select variables for the email address from the *Add placeholder* list.
d. In the *Bcc* box, enter the email address of each undisclosed recipient that you want to send alert notifications to, or select variables for the email address from the *Add placeholder* list.
e. In the *Subject* box, enter the subject of the alert notification, or select variables for the subject from the *Add placeholder* list.
f. In the *Message* box, enter the message for the body of the alert notification, or select variables for the message from the *Add placeholder* list.
g. Select the *Add Attachment* check box to add an attachment to the alert notification.
h. Under *File Name*, select *Use Automatically Generated Name* or *Use Specific Name*. If you select *Use Specific Name*, enter a file name or select a placeholder in the list.
i. Select the *Add File Extension* check box to automatically a file extension to file names.

   If you do not add a file extension to a file name, the document cannot be opened.

7. Click *Save & Close*.

Related Information

Locating alert source objects in the CMC [page 280]

24 Profiles

24.1 Creating a profile

1. Go to the *Profiles* management area of the CMC.
2. Select *Manage* > *New* > *New Profile*.
3. In the *Create New Profiles* dialog box, enter a name for the profile in the *Title* box.
4. Enter a description of the profile in the *Description* box, and click *OK*.

24.2 Specifying a global profile target for a profile

Local profile targets are specified during the publishing process.

1. Go to the *Profiles* management area of CMC.
2. Locate and select the profile to which to specify a profile target.
3. Select *Actions* > *Profile Targets*.
4. In the *Profile Targets* dialog box, click *Add*.
5. Select a universe in the *Universe Name* list.
6. Enter a class name in the *Class Name* box, or click *Select object from the universe*.
7. Enter a variable name in the *Variable Name* box, or click *Select object from the universe*.
8. Click *OK*.

24.3 Specifying a profile value for a user or group

You can achieve the same result by starting with the profile for which specify a value

You can use different types of profile values—for example, a static profile value or expression or variable profile values for third-party users and groups that are mapped to the system.

1. Go to the *Profiles* or the *Users and Groups* management area of CMC.
2. Select the profile for which specify a value, or select the user or user group for which to specify a profile value.
3. Select *Actions* > *Profile Values*.
4. In the *Profile Values* dialog box, click *Add*.
5. Click *Choose*.

6. Select a user or group or multiple users or groups, and click > to move them into the list on the right side.
7. Click *OK*.
8. Enter a profile value for the selected user or group or multiple users or groups.
   - To add a value, click *Value*, enter a value in the *New Value* box, and click *Add*.
     You can add multiple static values for a user or group and use **%NULL%** as a static profile value if a user or group does not have values that the profile can filter for personalization.
   - To use a filter expression, click *Filter Expression*, and enter an expression in the *Web Intelligence formula expression* box or the *Crystal reports expression* box. To apply the profile to multiple document types, enter filter expressions in all three boxes.
     To use a Web Intelligence expression, first specify a global profile target for the profile.
9. Click *OK*.

Related Information

Using variables as profile values [page 286]

24.4 Using variables as profile values

When adding a user or user group to a profile, you can specify a variable profile value for a user's full name, account name, or email address.

The following table describes the placeholder variables that you can use to externalize profiles:

Variable	Description
Title	Associated with the account name of a user or user group
User's full name	Associated with the full name of a user or user group
E-mail address	Associated with the email address of a user or user group. When you map the *E-mail address* variable to a common email address for a user group, the BI platform resolves the variable and retrieves individual email addresses for each member of the group.

1. Go to the *Profiles* management area of CMC.
2. Locate and select the profile to which to add the user or user group.
3. Select *Actions* > *Profile Values*.
4. In the *Profile Values* dialog box, click *Add*.
5. Click *Choose*.
6. Select a user or user group from the list on the left, and click > to move the user or group to the list on the right.

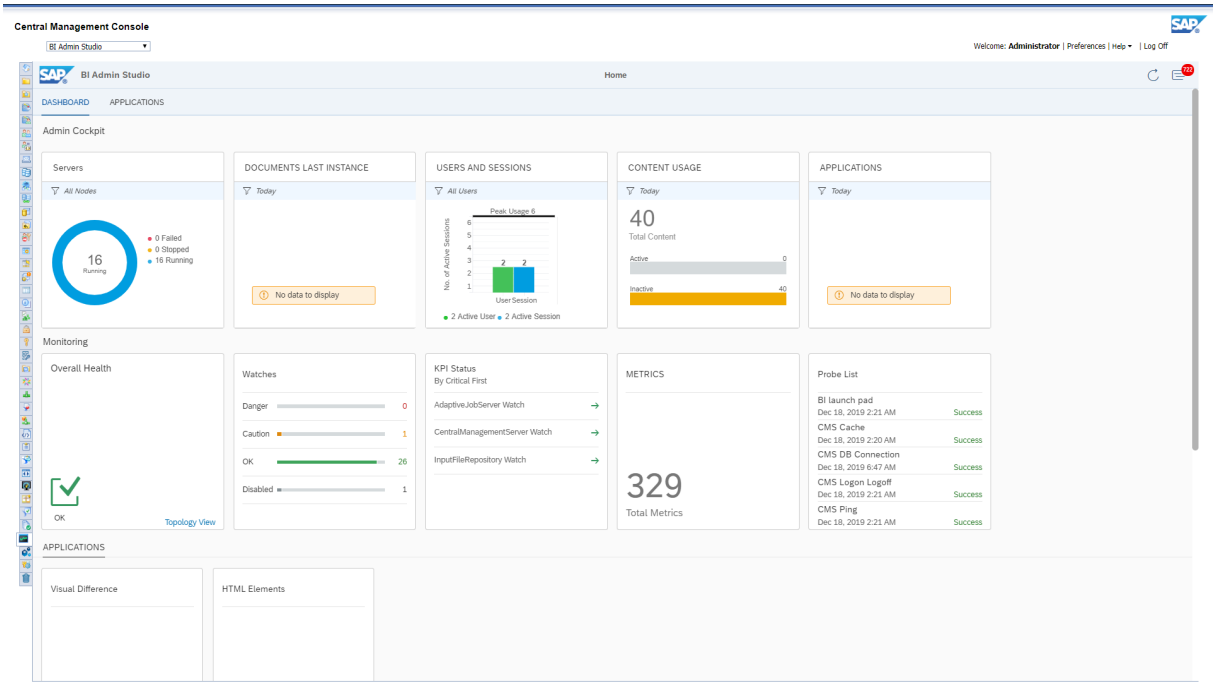
7. Click *OK*.
8. Click *Value*.
9. Select a placeholder variable in the *Add placeholder* list, and click *Add*.
   The placeholder appears in the *Existing values* box.
10. Click *OK*.

When you use the profile to personalize a publication, the profile value for the third-party user will update itself with the most recent user information. For example, if the user's email address has changed since the last time the publication was run, the email address used for the profile value will change the next time the publication runs.

25 About 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 About Admin Cockpit [page 289] and to learn more about Monitoring, refer to About Monitoring.

Applications

You can access *Visual Difference* and *Authorized HTML Elements* from the *Applications* tab. For more information on *Visual Difference*, refer to Visual Difference in the promotion management tool [page 318] and to learn more about *HTML Elements*, refer to Authorizing HTML elements.

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.

25.1 About 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.

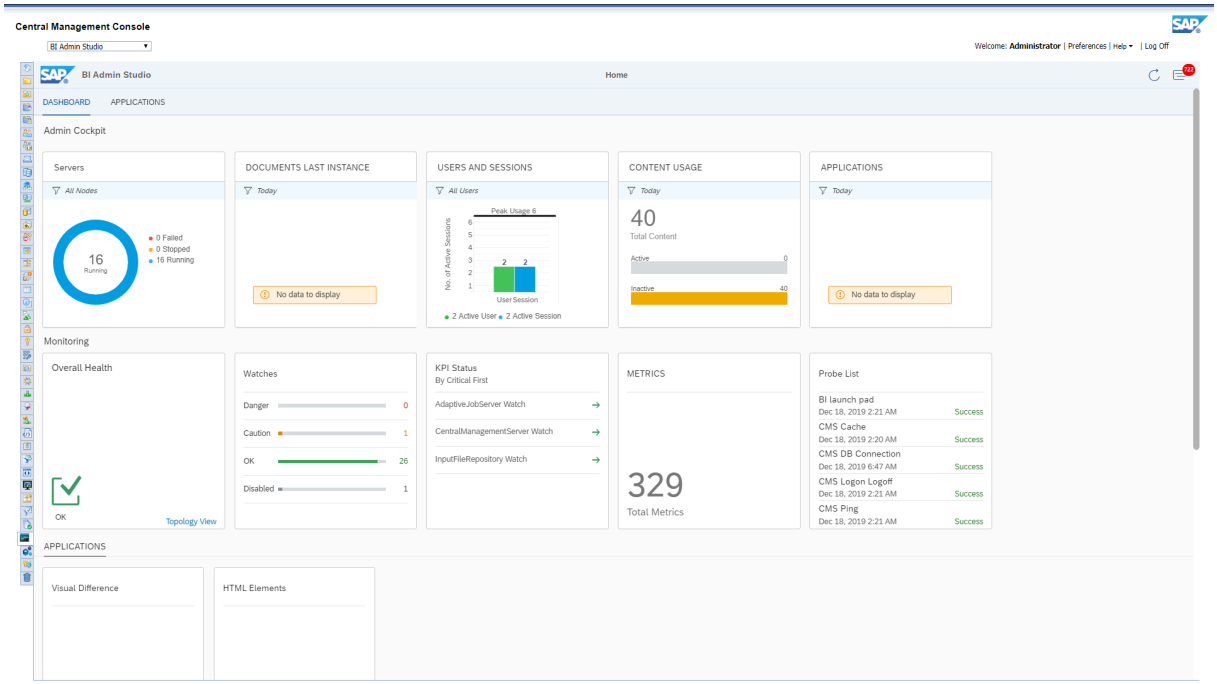
> **Note**
>
> The following requirements are necessary to ensure that the Admin Cockpit can be used successfully:
>
> - Monitoring service must be enabled.
> - Audit and relevant event must be enabled so that correct data is fetched.
> - BI platform RESTful Web Service must be accessible by clients.
> - WACS must be running, unless RESTful Web Service is deployed on Tomcat.
> - If you configure SSL for CMC, make sure to also configure SSL for WACS, unless RESTful Web Service is deployed on Tomcat.
> - 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.

25.1.1 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.

25.1.2 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 hage provides you with the following details:

- Total number of servers
- Number of error producing servers
- 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*.

25.1.3 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.

25.1.4 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*.

25.1.5 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.

> **i 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.

25.1.6 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*.

25.2 Monitoring

The monitoring application in SAP BusinessObjects Business Intelligence Platform provides the ability to capture the runtime and historical metrics of BI platform servers for reporting and notification. The monitoring application covers the activity of indicating that the application is functioning normally.

The monitoring application can be accessed from the CMC home page. The monitoring application consists of the following tabs:

- *Dashboard*: contains the Overall Health Status, KPI Status, Watchlist Status, recent alerts and quick links.
- *Metrics*: lists all the metrics found in the BI platform system. Provides option for creating a new Metrics.
- *Watchlist*: lists the number of watches by status such as *Danger*, *Caution*, *OK*, *Disabled*, and *Failed*.
- *Probes*: lists the probes along with their status and the corresponding graphs.
- *Alerts*: lists all the alerts generated by the monitoring application.

25.2.1 Dashboard

The Dashboard page enables the user to keep track of the system's health from a single screen. It provides real-time information about KPIs, recent alerts, and health of the BI deployment.

25.2.1.1 Dashboard Alerts

The *Recent Alerts* pane in the dashboard displays a maximum of six recent alerts, and the times when the alerts were recorded. You can click an alert to view the possible cause of the problem and action taken. Click the Alerts tile header to go to the *Alerts* page.

> **Note**
>
> The cause and action appear only if they were recorded when an alert was confirmed.

For more information on the activities you can perform on the *Alerts* page, see Alerts [page 317].

25.2.1.2 Dashboard KPIs

25.2.1.2.1 Customizing the KPI Status Pane

The *KPI Status* pane displays KPIs based on your choice. You can customize the KPIs to be displayed on the *KPI Status* pane by performing the following steps:

1. Click *Select KPI*. You can see the list of KPIs available for selection.
2. Select the KPIs that you need to view in the *KPI Status* pane. You can select up to eight KPIs here. To remove a KPI, unselect it from the dropdown list. Click the KPI tile header to go to the *Watchlist* page from where you can add or remove KPIs.

> **Note**
>
> You can view the recent updates related to the KPI by clicking the *Recent Update* link from the KPIs displayed in the KPI Status pane.

25.2.1.2.2 Achieving a Root Cause Analysis from the KPI Status Pane

You can utilize the KPI Status pane to identify the cause of failure of a metric.

1. Click any KPI displayed in the *KPI Status* pane.
   The *Watch Details* screen appears.
2. In the *Watch Details* pane, go to *General Properties* and *Watch Rule* to view the root cause of failure or success of a metric.

25.2.1.3 Overall Health Status Indicator

The *Overall Health* pane provides an indication of the overall health status of the BI platform deployment.

Example: If the health status of any of the Service Categories, Enterprise Nodes, or Server Groups is red, the overall health status indicator is also red.

Click *Topology View* on the *Overall Health* pane to view the BI Platform deployment based on:

- Enterprise Nodes
- Server Groups
- Service Categories

Topology View

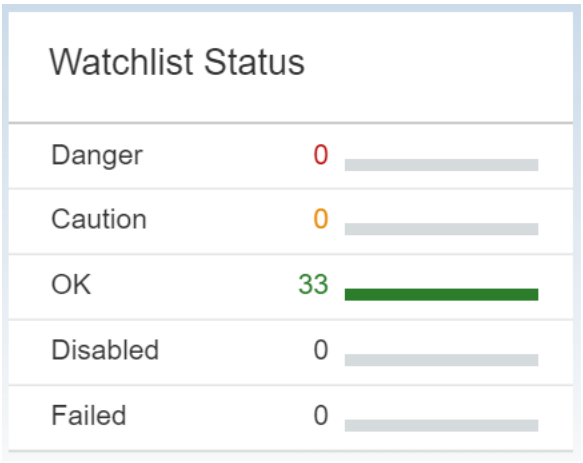
With the *Topology View*, you can:

- Display the selected BI Platform deployment in graphical or tabular format, by toggling the icon.
  - The inset window displayed with the graphical format depicts the immediate parent and peers of an expanded node after a drill-down. Click the inset window to go back to the parent node. In the case of server groups, you can view the root node of the hierarchy.
    With the graphical format, hover over each node to get the health status. Double-click a node to view the Watch Details of this node.
  - With the tabular view, the health status is visible in the *Overall Status* column.
- Filter the deployment by type with the *Show Type* dropdown list.
- Filter the selected deployment by state with the *State* dropdown list.
- Retrieve the latest health status by clicking the *Refresh* icon in the *Filter Panel*.

25.2.1.4 Watchlist Status

The *Watchlist Status* indicates the overall Watch count, and displays the number of Watches in each state:

- Danger
- Caution
- OK
- Disabled
- Failed



25.2.1.5 Quick Links

The *Quick Links* tile allows you to directly perform the following tasks from the Dashboard:

- *Create New Metric*
- *Create New Watch*
- *Create Java-based Probe*
- *Create Script Probe*

25.2.2 Graphs

Graphs in the monitoring application enable you to monitor the system performance at different time intervals. On the Probes page, the graphs are based on the roundtrip time and probe status. On other pages, graphs are based on the metric data.

> **i Note**
>
> The time displayed in the graphs is the time that is set in the *Time Zone* field in *CMC Preferences*. If you select *Default - Local to web server*, then the time zone of the location of the server is taken.

Graphs can be viewed in the following two modes:

- Live mode: This mode displays the probe status for the last 2 minutes and is continually updated. Histogram, Zoom In, Zoom Out, and Calendar options are disabled in this mode.
- History mode: This mode enables you to view graphs with historical data. Histogram, Zoom In, Zoom Out, and Calendar options are enabled in this mode. You can view the graph for a maximum of 6 months in the History mode.

The main areas in the graph are as follows:

- Header - displays the metric title and the mode along with the time range for which the graph is being displayed. The header also displays the current value in the Live mode.

- Main Graph - displays the current state of the metric or probe run along with the date and time.
- Toolbar - the toolbar contains the following buttons:

: this toggle button enables you to switch between Live and History modes.

: the calendar option enables you to select the start and end time and date.

: enables you to view the graph in full screen.

Synchronizing the Time axis

Synchronizing time axes is a functionality provided for graphs in the monitoring application. When viewing multiple graphs in the same window, you can click *Synchronize Time Axes* to set the same time range for all the graphs. When you change the time range in one graph, the time range in all the graphs changes accordingly. Synchronizing time axes works in both History and Live modes.

25.2.3 Probes

A probe is a utility that provides the ability to monitor the SAP BusinessObjects system using a simulated application. The results and graphs generated by these probes provide valuable input for system availability, health, and stability, and performance statistics of different SAP BusinessObjects services and functionalities. This data can also be used for capacity planning.

You can run a probe to check the system health at any given time. Probes can be scheduled to run at specified intervals. You can have more than one schedule for a single probe. When a probe is run, the probe result and the roundtrip time are displayed and are also represented graphically. Metrics generated by probes are called virtual metrics. These virtual metrics can be used while creating watches.

You can use the BI platform monitoring probes to perform the following activities:

- Simulate end user workflows, such as user login actions and report execution of Web Intelligence and Crystal Reports applications.
- Test the availability, functionality, and performance of SAP BusinessObjects services.
- Test the Central Management Server (CMS) core functionality, CMS cache service, and CMS database connection.

Probes can be used in the following scenarios:

- To check the load on the CMS, you can run the CMS Database Connections probe. Using the probe result and roundtrip time at different intervals of time, you can plan a deployment, or schedule large-scale report production effectively.
- To check availability of a server, you can run one of the CMS probes at different intervals of time and know the server traffic at any given time.

25.2.3.1 Types of Probes

Probes can be classified into:

- Diagnostic probes: Probes that generate reports containing current system information. Examples of diagnostic probes include Stop/Start Server. This probe checks all the servers, records the state of each server, restarts the servers and collects information about servers again.
- Health probes: Probes that generate metrics of data types such as integer, Boolean, or string. Examples of health probes include CMS Logon/Logoff. This probe checks whether users can log on and log off from the Central Management Server (CMS) successfully.
- Hybrid probes: Probes that function as both diagnostic and health probes. Except for Stop/Start Server probes, which are diagnostic probes, all other probes provided with the BI platform are hybrid probes.

By default, the following monitoring probes are shipped with the BI platform:

CMS Logon/Logoff

The CMS Logon/Logoff probe tests the availability of the CMS and the ability of users to log into the system through client applications. The probe logs in as a user, checks the session validity, and then logs out.

Crystal Reports Service Through Page and Cache Server

The Crystal Reports service through the Page and Cache server probe tests the availability of the Crystal Reports service through Crystal Reports Page servers and Cache servers. The probe uses the Crystal Reports Page and Cache servers to open a report, optionally refresh the report, optionally export the report to PDF format, and close the report.

Crystal Reports Service Through Report Application Server

The Crystal Reports service through the Report Application Server probe tests the availability of the Crystal Report service through Report Application servers. The probe uses the Report Application Servers to open a report, optionally refresh the report, optionally export the report to PDF format, and close the report.

Web Intelligence Service

The Web Intelligence service probe tests the availability of the Web Intelligence service through the Web Intelligence Report servers. The probe opens a Web Intelligence document, optionally refreshes it, optionally exports the document to XLS and PDF formats, and closes the document.

CMS Ping

The CMS ping sends an empty query to the CMS. This probe is considered successful if the CMS returns a parse failure error. This probe is expected to complete quickly because query parsing is part of the CMS core functionality.

CMS Cache

The CMS cache probe tests the availability and health of the CMS cache by sending the following query:

```
select SI_NAME from
          CI_SYSTEMOBJS where SI_OBTYPE=4
```

This query returns the system InfoObject that contains the CMS cluster name. The CMS retrieves the system InfoObject from the cache rather than the repository database. If the cache is not functioning properly or if the cluster definition is incorrect, the query fails.

CMS Database Connection

The CMS Database Connection probe tests the availability of the repository database by executing the following query:

```
select SI_NAME from CI_SYSTEMOBJS
          where SI_OBTYPE=13
```

This query returns the system InfoObject, which is the User desktop plugin object. The CMS retrieves the system InfoObject from the repository database. If the connection between the CMS server and the repository database is not proper, the query fails.

BI launch pad

The BI launch pad probe checks the basic health of BI launch pad. This involves logging into BI launch pad with a selected authentication type (such as Enterprise, LDAP, SAP, or Windows AD), and logging out.

Note these limitations:

- If BI launch pad is configured to hide the authentication method during login, the authentication type that is selected on the probe's properties page is ignored.
- If you have set up a custom entry point to BI launch pad (another web page that redirects the BI launch pad logon page; for example, a `http://localhost:8080/BOE/BI/custom.jsp` page that redirects to `http://localhost:8080/BOE/BI`), then do not use the custom entry point with the BI launch pad probe.
- On the properties page for the BI launch pad probe, the "Infoview application name" setting is not used (it is deprecated).

Stop/Start Servers

The Stop/Start Servers probe checks the status of servers that the user wants to check. This involves stopping and starting the servers to be monitored.

25.2.3.2 Managing Probes

The *Probes* page of the monitoring application displays all the probes along with the schedule status, the next scheduled run, and the previous run result with time. There are two graphs displayed when a probe is selected: *Result* and *Roundtrip Time*. By default, these graphs are in History mode. On the *Probes* page, you can run a probe, schedule a probe, check the properties or history of the probe, set probe limits, and refresh probes.

To set probes to be refreshed automatically, click . If you want to manually refresh a probe, click .

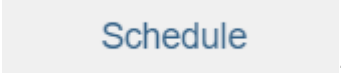
25.2.3.2.1 To Run a Probe

You can run a probe whenever you want. Select a probe from the list of probes and click *Run Now* . When the probe is running, the *Previous Run Result and Time* column displays the status of the probe as *Running* and displays the time when the probe run was initiated. When the probe completes its activities, the *Previous Run Result Time* column displays the roundtrip time in milliseconds, and the probe initiation date and time. Graphs for the Result and Roundtrip Time of the probe are displayed.

> **i** Note
>
> The status of a probe can be Success, Failure, or Timed Out. Click on the probe status to view the probe result details. The status `No data available` is displayed if the probe was never run or if the probe data was deleted.

25.2.3.2.2 To Schedule a Probe

You can schedule individual probes to run at specified times. To schedule a probe:

1. Select a probe from the *Probe* column, and then click 

.
2. Click *Recurrence* in the left pane of the *Schedule* dialog box that appears, and select a recurrence pattern from the *Run Object* drop-down menu.
   When you select a recurrence pattern, the application prompts you to provide additional information. The following table lists the additional information you must provide for each recurrence pattern:

Run Object Options	Additional Information Required
Now	None
Once	Define the start and end date/time
Hourly	Define the hour and minute, and then define the start and end date/time
Daily	Define the number of days, and then define the Start and End date/time
Weekly	Select the days of the week, and then define the start and end date/time
Monthly	Define the number of months, and then define the start and end date/time
Nth Day of month	Select the day of the month, and then define the start and end date/time
1st Monday of Month	Define the start and end date/time
Last Day of Month	Define the start and end date/time
X Day of Nth Week of the Month	Select the week and the day, and then define the start and end date/time
Calendar	You can select a customized calendar, and then define the start and end date/time.

3. Enter the number in the *Number of retries allowed* and the required time in the *Retry interval in seconds* fields.
4. Click *Schedule For* and based on your requirements, select either *Schedule only for myself* or *Schedule for specified users and user groups*.
   If you select *Schedule for specified users and user groups*, the application prompts you to provide the name of the user or user group. Select the users or the user group from the list provided in the *Available* column and click . Click to remove the user group from the selection.
5. Click *Schedule*.

Default Scheduling

Default scheduling settings enable you to run multiple probes on a similar schedule. To define default scheduling settings proceed as follows:

1. Select a probe from the *Probe* column, and then click *Schedule*.
2. Click *Default Settings*.
3. Follow the same steps as for scheduling individual probes.

25.2.3.2.3 To View Probe Properties

The *Probes* page allows you to view the properties of probes as well as to modify certain fields. All probes have some general properties and certain properties specific to each probe. To view and modify the properties of a probe, proceed as follows:

1. Select a probe and click *Properties*.
2. Modify the fields according to your requirement and click *Save & Close*.

The following table lists the general properties of probes:

Parameter	Description	Type
Title	Title of the probe	String
CUID	CUID of the probe	
Description	Brief description of the probe functionality	String
Created	Date and time when the probe was created	
Last Modified	Date and time when the probe was last modified	
Last Run On	Date and time when the probe was last run	
Timeout (sec)	Time limit (in seconds) after which the probe execution stops	Integer

The following tables list the input parameters required for specific probes:

Crystal Report service through Page and Cache server

Input Parameter	Description	Type
CUID	CUID of the document	String
export	If you select True, the document is exported to PDF format If you select False, the document is not exported to PDF format	Boolean
refresh	If you select True, the document is refreshed If you select False, the document is not refreshed	Boolean

Crystal Report service through Report Application Server

Input Parameter	Description	Type
CUID	CUID of the document	String
export	If you select True, the document is exported to PDF format If you select False, the document is not exported to PDF format	Boolean

Input Parameter	Description	Type
refresh	If you select True, document is refreshed If you select False, document is not refreshed	Boolean

BI launch pad

Input Parameter	Description	Type	Example Value
Authentication type	Authentication type	String	Enterprise
CMS name	Name of the CMS used in the BI launch pad application	String	localhost:6400
Password	BI launch pad password	String (encrypted)	Password1
URL base	Base URL of the BI launch pad application to which the user connects	String	http://localhost:8080/BOE/BI
User name	BI launch pad username	String	Administrator

Start Stop Servers

Input Parameter	Description	Type	Example Value
where-clause	This input parameter enables the user to define which servers are to be monitored	String	`Where SI_PROGID='CrystalEnterprise.Server' AND SI_SERVER_KIND NOT IN ('aps') AND SI_NAME NOT LIKE '%AdaptiveProcessingServer%' AND SI_NAME NOT LIKE '%AdaptiveJobServer%'`

Web Intelligence service

Input Parameter	Description	Type
CUID	CUID of the document	String
pdfexport	If you select True, the document is exported to PDF format. If you select False, the document is not exported to PDF format	Boolean
refresh	If you select True, the document is refreshed If you select False, the document is not refreshed	Boolean
xlsexport	If you select True, the document is exported to excel format If you select False, the document is not exported to excel format	Boolean

25.2.3.2.4 To View the Probe History

The monitoring functionality logs the results of probes that are run. To view the history of a probe, select a probe from the *Probe* column, and then click *History*.

The *History* dialog box appears, listing the probe run instances. The History dialog box provides the following details for all the instances:

Field	Description
Instance Time	Displays the time when the probe was initiated
Title	Displays the title of the probe
Status	Displays whether the schedule was successful
Created By	Displays who has created the probe
Type	Displays the type of probe. For example, diagnostic or health or hybrid.
Run Result	Displays whether the probe yielded a positive, negative, or no result

You can perform the following actions in the *History* dialog box:

- To refresh the list of instances, click on or click on *Manage* and select *Refresh*.
- To delete an instance, select the instance, click on *Manage*, and select *Delete*.
- To view the details of an instance, select the instance and click . The *Instance Details* opens in a separate window.
- To pause an instance or resume a paused instance, select the instance and click on *Actions* and select *Pause* or *Resume* appropriately. You can also use the icons provided.
- To re-run an instance, select the instance and click or click *Actions* and select *Run Now*.

  > **i** Note
  >
  > You can use the filters provided for the *Instance Time*, *Title*, *Status*, and *Created By* columns.

- To view the probe result details, click on the result of a probe. The *Probe Result* dialog box opens. The *Probe Result* page displays the following:

  Probe Name
  Result
  Duration
  Diagnostic Messages

25.2.3.2.5 To Set Schedule Limits

The probe limits feature enables you to manage probe instances. You can use this feature to specify the number of instances that must be displayed in the *History* dialog box or the number of days for which you

want to keep the historical instances. After you set the number of instances or the number of days, the excess instances will be deleted from the database. To set the limits on probe history, proceed as follows:

1. Select a probe from the *Probe* column, and then click *History*.
2. In the left pane, click *Limits*. In the Limits dialog box, select the *Delete excess instances when there are more than N instances of an object:* and enter the required number.
3. If you want the instances limit that you set to be applied only to selected users or user groups, click *Add* against *Delete excess instances for the following users/groups*. Select the users or user groups from the *Available users/groups* and click or click to select all the users and user groups.
4. If you want the instances limit for the number of days to be applied only to selected users or user groups, click *Add* against *Delete instances after N days for the following users/groups*. Select the users or user groups from the *Available users/groups* and click or click to select all the users and user groups.

25.2.3.2.6 Managing Probes Through the Command Line

The BI platform monitoring application lets you add, run, and delete a probe through the command-line interface (CLI).

> **Note**
>
> For each parameter definition, the format is `<name>:<type>:<value>`, plus an optional fourth parameter: `true`, to encrypt the value. If `true` is specified, the value will be encrypted in the Central Management Server database, and it will also be masked in the probe's properties page in the Central Management Console.

> **Note**
>
> The command syntax uses colons and semicolons as delimiters; therefore, you cannot set a parameter such as `urlbase` to be `localhost:8080`. You need to first create the probe, then use the CMC to set the URL for the probe.

Adding a New Probe Through CLI

1. Enter the following path in the command-line interface: `cd C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\win64_x64\scripts`.
2. Enter the **`probeAdd`** command along with the required attributes and parameters as described in the following table:

Attributes/Parameters	Description	Example
`-auth`	Authentication type (for ADDING the probe)	secEnterprise
`-classname`	Fully qualified class name of the probe	-classname com.businessobjects.monitoring.probe.ProbeInfoView
`-cms`	CMS Name	localhost:6400
`-help`	Print help for this application	
`-inputparam`	Input parameters for the probe given	-inputparam "authtype:string:enterprise;urlbase:string:localhost;cmsname:string:host_machine_name;username:string:administrator;password:string:Password1:true"
`-name`	Name of the probe	BI launch pad
`-password`	Password (for ADDING the probe) (case-sensitive)	Password1
`-timeout`	Timeout interval in seconds	10
`-username`	User name (for ADDING the probe)	Administrator

> **i** Note
>
> The parameters `-auth`, `-username`, and `-password` above are used to ADD a probe. The authentication type, user name, and password for RUNNING the probe are contained within the `-inputparam` parameter.

Running a Probe Through CLI

1. Enter the following path in the command-line interface: `cd C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\win64_x64\scripts`.
2. Enter the **`probeRun`** command along with the required attributes and parameters as described in the following table:

Attributes/Parameters	Description	Example
`-auth`	Authentication type	secEnterprise
`-cms`	CMS Name	localhost:6400
`-cuid`	CUID of the probe	
`-help`	Print help for this application	
`-id`	ID of the probe	
`-name`	Name of the probe	BI launch pad

Attributes/Parameters	Description	Example
`-password`	Password to run the probe (case-sensitive)	Password1
`-resultdir`	Directory to dump the probe result	C:\proberesults
`-username`	User name to run the probe	Administrator

> **Note**
>
> When running a probe, you must provide only one of the following parameters: `-cuid`, `-id`, `-name`. If more than one of these parameters is provided, an error occurs.

Deleting a Probe Through CLI

1. Enter the following path in the command line interface: `cd C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\win64_x64\scripts`.
2. Enter the **`probeDelete`** command along with the required attributes and parameters as described in the following table:

Attributes/Parameters	Description	Example
`-auth`	Authentication type	secEnterprise
`-cms`	CMS name	localhost:6400
`-cuid`	CUID of the probe	
`-help`	Print help for this application	
`-id`	ID of the probe	
`-name`	Name of the probe	BI launch pad
`-password`	Password to delete the probe (case-sensitive)	Password1
`-username`	User name to delete the probe	Administrator

> **Note**
>
> When deleting a probe, you must provide only one of the following parameters: `-cuid`, `-id`, `-name`. If more than one of these parameters is provided, an error occurs.

25.2.3.2.7 Adding New Probes

The BI platform monitoring application is shipped with several default probes. In addition to these default probes, you can create your own customized probes and add them to the monitoring application. You can create a new probe by using the provided SDKs.

For more information about creating a new probe, see the *SAP BusinessObjects Java Developer Guide*.

25.2.3.2.8 Registering Java Based Probes

You can register Java based probes by completing the following steps:

1. From *Probes*, select , then Java Based Probe .
   The *Register Probes* screen appears.
2. Enter the details in the *Probe Name*, *Description*, *Timeout* and *Classname* fields.

   > **Note**
   >
   > In the *Classname* field, enter the complete class name including the package name. For example, `com.businessobjects.monitoring.probe.CMSLogOnOffProbe`.

3. Select the *Probe Type*.
4. Click *Add* to specify the input parameters such as the user name and password required to run the probe. The name and type of these input parameters should be consistent with that of the implementation class.

25.2.3.2.9 Registering Script-Based Probes

To register script-based probes, complete the following steps:

1. From the *Probes* tab, click *Register* > *Script Probe* .
   The *Probe Registration* window appears.
2. Enter the *Probe Name*.
3. Select the *Probe Input Type*. If the selected probe input type is Command Line, then enter the command in the *Command* field; otherwise browse and select the script file location in the *Script File* field.
4. To define a virtual metric, select the *Define Virtual Metrics* check box.
   - *Define Delimiter* - Specify here the delimiter to be used to parse the output. The administrator should ensure that the delimiter will correctly parse the output.
   - *Output type* - A probe can have either *Tabular Output* or *Key-Value* output. If you select *Tabular Output*, enter the *Metric Identifier Column* and *Metric Values Column Numbers*.

25.2.4 Watches

Watches provide real-time status and historical trends of servers and workflows within the BI platform environment. Users can associate thresholds and alerts to a watch. You can create a watch using the data from probe metrics, server metrics or a combination of both. Watches enable you to understand and improve the system functionality and performance of the BI platform environment.

At any given time, the traffic light associated with each watch indicates the watch state. You can set the number of states in a watch as 2 or 3.

- Number of states = 2: Only one transition takes place. When the set threshold of a watch is breached, the associated traffic light changes from green to red or vice versa.

- Number of states = 3: Two transitions take place and the associated traffic light changes from green to amber and then amber to red or in the reverse order.

You can view watches on the *WatchList* page as well as on the *Dashboard* page. On the *WatchList* page, you can view the list of watches along with critical information such as the watch state, type, description, and if the email notifications are paused or resumed. In the WatchList page only the server name is displayed. Position the cursor over the node to view the complete name of the server. When a watch is selected, a graph based on the metric data is displayed. This graph can be viewed in both Live and History modes; however, the graph is in Live mode by default. From the *Watchlist* page, you can create a new watch. You can also view the watch details, copy, edit, change email notification settings of an existing watch, suspend or resume email notifications, and add watches to favorites.

25.2.4.1 Types of Watches

Watches can be classified into:

- System watches: Watches that are shipped with the BI platform monitoring application. By default, there will be one system watch associated with each server type. You cannot delete a default system watch; however, you can customize these watches by changing the metrics and editing the threshold values. You can even copy these watches and create your own watch with different metrics and threshold values. You cannot modify the association of a watch with a server.
- User-created watches: Watches that you create. You can create a watch with metrics of your choice, and set threshold values and alerts. You can also copy a system watch and customize it to suit your needs. User-created watches can be deleted. You cannot associate a user-created watch with any server.

25.2.4.2 Creating a New Watch

You can create a new watch, either from the *Dashboard* page or from the *Watchlist* page. On the *Dashboard* page, click

and on the Watchlist page, click .

1. Go to the *Monitoring* area of the CMC and click the *Watchlist* tab.
2. Click and set the properties and options as described in the following sections:

> **i** Note
>
> The metric selected will appear by default in the *Added Metrics* area.

General Properties

On the *New Watch - General Properties* screen, you can define the *Name*, *Description*, *Number of States*, and *Settings*. To define the general properties, complete the following steps:

1. Enter the name and description in the appropriate fields.
2. Select *Number of States* to set the number of thresholds.
   If you select two states, the watch state changes from green to red or vice versa. If you select three states, the watch state changes from green to amber, amber to red, or the reverse order.

   > **i Note**
   >
   > Select *Write to Trending Database* for the watch result to be stored on the trending database. You can view trending graphs from this data.

3. Click *Step 2*.

Caution Rule

On the *New Watch - Caution Rule* screen, you can add metrics, set the threshold values, and view the current state of the watch that you are creating. To set the caution settings, complete the following steps:

1. Select metrics in the *Available Metrics* pane and click .
   The *Filter* option enables you to search metrics of your choice from the existing list.
   By default, the Boolean operator for two metrics is `(AND) &&`. You can change the Boolean operator to `(OR) ||` by using the drop-down list below the metric. After adding the metrics, the Boolean expression of the metrics added is displayed. You can edit the Boolean expression. The Boolean expression must be of the format `NodeName.ServerName$'MetricName'>=ThresholdValue`. The following is an example of a boolean expression:

   ```
   <Node_name>.CentralManagementServer$'Completed Jobs'>=1
   ```

2. Select the operator from the drop-down list and then set the threshold value.
   The following table provides the available operators that you can use to set the threshold value:

Operators	Description
>=	Greater than or equal to
<=	Less than or equal to
>	Greater than
<	Less than
==	Equal to
!=	Not equal to

   Click to view the current expression state.

3. Click *Step 3*.

Danger Rule

The *New Watch - Danger Rule* screen appears only when the number of states selected is three. On the *New Watch - Danger Rule* screen, you can add metrics, set the threshold value, and view the current state of the

watch that you are creating. By default, the values provided for caution settings are retained in the danger rule screen. If you need to retain the same metric, you must modify the operator or threshold value. You can also delete these metric settings. To set the danger settings, complete the following steps:

1. Select metrics in the *Available Metrics* pane and click .
2. Select the operator from the drop-down list and then set the threshold value. Click to view the current expression state.
3. Click *Step 4*.

Throttle and Notification

On the *New Watch - Throttle and Notification* screen, you can choose to enable email notifications and set how you want the watch state to be shown on the *Dashboard* and *Watchlist* pages. You can either choose to change the watch state for every threshold breach or set throttling conditions for it.

1. If you want the watch state to change for every threshold breach, select *Change watch state every time Caution or Danger Rule evaluates to true*. Whenever a caution or danger evaluates to true, the watch state changes to the corresponding state. If both caution and danger rules evaluate to true, then the watch state changes to red.
2. If you want the watch state to change according to a throttling condition, select *Change watch state according to Throttling criteria below* and provide the required *Caution Throttling Criteria* and *Danger Throttling Criteria* settings as described below:

   Choose *If Rule evaluates to true for last:* and provide the required time duration. The time duration can be in days, hours, minutes, or seconds. For example, if you choose this option and set a time duration of 5 minutes for the caution rule and if the caution rule evaluates to true, the watch state changes to amber. Similarly, you can set the rule for Danger. If both caution and danger rules evaluate to true, the watch state changes to red.

   If you want the watch state to change only after a specific number of breaches in a particular time, choose *Wait for __ true evaluations in the last:* and provide the number of true evaluations and set the time duration. For example, if you set the number of true evaluations to 20 and the duration to 5 days, the watch state will change only when the number of true evaluations exceeds 20 in 5 days. If both caution and danger rules evaluate to true, the watch state changes to red.
3. If you want any actions to be performed when the watch state changes, select *Configure Action*, and then select an appropriate probe from the *Run Probe* dropdown list. For example, if you created a watch with three states, you can configure a probe to be executed when the watch state is amber, and also when the watch state changes to red.
4. Select *Enable alert notifications* in *Notification Settings* to enable alerts.
   Alerts are generated based on changes of the watch state:

Previous Watch State	Current Watch State	Alert Generated?
Green	Red	Yes
Amber	Red	Yes
Green	Amber	Yes
Red	Green	NA

Previous Watch State	Current Watch State	Alert Generated?
Amber	Green	NA
Green	Green	NA
Amber	Amber	No
Red	Red	No
Red	Amber	No

5. Click *Directory*. The Directory page opens.
6. If you want to add individual e-mails, enter the e-mail ID and click *Add email recipient* or select the user or group name from the table, click *Alert Settings*, and select the required options.
7. If you require detailed information about the metrics that caused the alert, select *Add Metric Trend History As Attachment*. A graph of historical metrics data will be appended to the alert. The graph contains data for 10 minutes, starting from when the alert was triggered.
8. Click *Review* and then click *Save* to complete the creation of a new watch.

> **i** Note
>
> You can copy the *Caution Throttling Criteria* by clicking the check box of Apply Caution Criteria in *Danger Throttling Criteria*.

25.2.4.3 Managing Watches

The *Watchlist* page of the monitoring application displays all the watches along with the status, type, and description of all the watches. When a watch is selected, a graph based on the metric data is displayed. You can view all watches, or filter watches based on their state, or display watches that are added as favorites by using the *Show* option. For example, to view watches that are KPIs, select *Show* > *KPIs*.

On the *Watchlist* page, you can edit a watch, copy or delete a watch, check watch details, enable or disable email notifications, add watches to favorites, and refresh the watches.

Email Notifications

You can enable or disable email notifications for a particular watch by using the *Email Notifications* button. The *Attributes* column indicates whether the email notification for a watch is paused or resumed.

Adding a Watch to Favorites

You can click the *Add to Favorites* button to add watches to your favorites list. You can then view only your favorite watches by selecting *Favorites* in the *Show* list. The watches that you add as favorites are user-specific and cannot be viewed by others who have logged in as a different user.

Refreshing watches

You can use *Enable Auto-Refresh* when you want the watches to be refreshed automatically, or you can also manually refresh the watches by clicking .

25.2.4.3.1 Editing a Watch

You can edit a watch and customize it as required. However, you cannot change the server association of the watches. Perform the following steps to edit a watch:

1. Select a watch from the list of watches and click .
2. Select a tab from the header panel to edit details related to the selected tab:

Options	Description
General Properties	You can edit information related to Name, Description, Number of States, and Settings of the selected watch.
Caution Rule	You can edit the Caution Rule information related to Available Metrics, Added Metrics, and Current Watch State.
Danger Rule	You can edit the Danger Rule information related to Available Metrics, Added Metrics, and Current Watch State.
Throttle and Notification	You can edit information related to email notification.

3. Click *Save*.

25.2.4.3.2 To Copy or Delete a watch

To Copy a Watch

The monitoring application provides the option of copying a watch. When you copy a watch, a new watch is created with the same information and settings. The new watch is copied with the same name with a number appended. For example, if you copy a watch named AdaptiveJobServer Watch, a new watch with the name AdaptiveJobServer Watch(2) is created.

To copy a watch, select a watch from the list of watches and click *Copy*.

> **i** Note
>
> Every default watch is associated with a server and when you copy a watch, the server association is removed from the copied watch.

To Delete a Watch

Default watches cannot be deleted; however, you can delete a user-created watch. To delete a user-created watch:

1. Select the watch and click *Delete*.
2. Click *OK* in the *Delete* confirmation dialog box.

You can also delete multiple watches simultaneously by selecting several watches and clicking *Delete*.

25.2.4.3.3 Viewing Watch Details

1. Select a watch and click *Details*.
2. The *Watch Details* dialog box displays the General Properties and the Watch Rule of the selected watch:

Options	Description
General Properties	Provides information related to the Watch Name, Watch Status, Watch Description, Read and Unread Alerts, Latest Alert, Caution Settings, Danger Settings, and Inbox Subscribers.
Watch Rule	Provides information related to the current state of metrics used in caution and danger settings, and a graph based on the metric state. You can view the graph in the Live or History mode.

25.2.4.3.4 Disabling a Watch

There are many watches in the BI platform monitoring application. You have the option of disabling a watch and if required it can be enabled again. When a watch is disabled, the watch state is not computed. Hence, if a watch is disabled for a set duration:

- The watch state will not show any data in the graph for that particular duration.
- Metrics that are a part of the disabled watch and not part of any other watch will also not display any data in the graph for that particular duration.

- Select the watch, click then *Disable Watch*.
- Click *OK* in the *Delete* confirmation dialog box.

You can also disable multiple watches simultaneously by selecting several watches and clicking *Disable Watch*.

> **Note**
>
> Only the administrator groups and the users who have created the watch will have the rights to enable or disable the watches.

25.2.4.4 Searching for a Watch

A search box is available on the Watchlist page that enables you to search for existing watches.

Searching for a Watch Based on Watch Name

1. Navigate to the *Watchlist* page.
2. Choose *Search by Watch Name* from the search combo box.
3. In the search box, enter the name of the watch you want to search for and click the search icon.

Searching for a Watch Based on Metric Name

1. Choose *Search by Metric Name* from the search combo box.
2. Type the metric name in the search box and click the search icon.

25.2.5 Metrics

The Metrics page displays all the metrics generated from the probes and servers. You can select metrics from the left panel to view them in the *View Selected Metrics* pane. The *Search* option enables you to view only the required metrics.

> **i** Note
>
> Metrics generated from the default probes are `execution time` and `passed`. The probe result is represented by the metric `passed` and has one of the following values:
>
> - 0, indicates the probe has failed.
> - 1, indicates the probe has passed.
> - 2, indicates the probe has timed out.
>
> However, users can define any number of metrics to be displayed when creating a new probe. These metrics are called virtual metrics. For a detailed list of server metrics, see the *Server Metrics Appendix*.

The *View Selected Metrics* pane displays the selected metrics along with the metric value and the date and time. Each selected metric also displays the graph, which you can choose to view in the Live mode or History mode. Select *Collapse All* to hide the graphs. Select *Synchronize Time Axes* to view multiple graphs with the same time range.

Server Metrics Through SAPOSCOL

Server level metrics, such as CPUcount, FreeMemory, and PhysicalMemory, can be viewed by installing SAPOSCOL. To get these metrics, enable host metrics in the Monitoring Application properties and provide

the path to where SAPOSCOL is installed. After enabling Host metrics, these metrics can be viewed in the Metrics page and in the Watch creation wizard. Select a server metric. The tooltip then displays the service name of this server metric.

Related Information

About the Server Metrics Appendix [page 475]

25.2.5.1 Derived Metrics

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.

Derived metrics can be viewed in the left pane on the *Metrics* tab.

25.2.5.1.1 Creating a Derived Metric

1. On the *Metrics* page or the *Dashboard* page, click *Create a Metric* or .
2. Enter the metric name and select a server from the left side panel.
3. Select metrics and click to add them to the metric formula.
4. Enter the operator in the metric formula manually. The supported operators are addition (+), subtraction (-), multiplication (*), and division (/).
5. To check if the metric formula is logically correct, click *Evaluate.*
6. Click *Step 2*.
7. Select *Metrics* > *Derived Metrics* > *OK*
8. Click *Review*.
9. Click *Save.*

> **i Note**
>
> You can save the metric only if the metric formula is logically correct.

The new derived metric appears under the appropriate server on the *Metrics* page.

25.2.5.1.2 Editing a Derived Metric

You can edit a derived metric formula; however you cannot edit the metric name or the server. Perform the following steps to edit a derived metric:

1. Select a metric in the left pane and click .
2. Revise the metric formula as desired.
3. To check if the metric formula is logically correct, click *Evaluate*.
4. Click *Step 2*.
5. Select *Metrics* > *Derived Metrics* > *OK*
6. Click *Review*.
7. Click *Save*.

25.2.6 Alerts

An alert is a notification generated by the monitoring application, when a user-defined expression or rule evaluates to true. Since a rule or expression can have multiple metrics and thresholds, the whole rule needs to be evaluated to true. You can choose either to receive alerts by e-mail or to view them on the *Dashboard* page. The alert e-mail will highlight metrics that have breached the threshold value and caused the watch to raise the alert.

You can enable alerts when you are creating a watch. For more information about setting alerts, see *Event Settings* in Creating a New Watch [page 309].

In the *Alerts* page, you can view all monitoring alerts along with the status of the alert, alert name, alert message, and the time the alert was generated. You can click on the alert name to access the *Alert Details* page containing the following information:

- Watch name
- Alert rating
- Time of alert
- Caution and danger rules along with the metrics and the metric values at the time of the alert

All alerts that are generated are in the *Unread* state and change to the *Read* state after you check the alert details. After you take action on an alert, you can change the status to Confirmed.

The following table lists the activities you can perform on the Alerts page:

Option	Description
Browse	Enables you to select a watch from the list and view the alerts generated by the selected watch.
Clear	Enables you to view the alerts generated by all watches.
Filter	Enables you to filter the alerts based on three states: *Read*, *Unread*, or *Confirmed*. **Note** The alert state is set to *Read* once you access the *Alert Details* page of that particular alert.

Option	Description
Confirm	Enables you to record the cause of the alert and the action taken to resolve it. Once action has been taken on an alert, you can set the alert to the *Confirmed* state. **i Note** Once you set the alert to *Confirmed*, the alert state is also marked as *Read*.
Delete	Enables you to delete an alert.

Reminder Alerts

You will receive reminder alerts if you have not responded to the first alert. For example, assume that an alert was sent after a watch reached its threshold. If you did not confirm the alert at the first instance it was sent, you will receive reminder alerts. On confirmation of a reminder alert of a watch, any previous alerts raised for the same watch are automatically confirmed.

25.2.7 Generating Reports for Monitoring data

You can use the "Monitoring TrendData universe", located in the `Universes>Monitoring TrendData Universes` folder, to generate reports for Monitoring. You can create intuitive reports to see information on Monitoring such as reporting Watch data, trending of watches, watch behavior over a period of time, probe trending, drill down on a watch to its metrics, and so on. To generate such reports, you need to install an SAP BusinessObjects desktop client, use the Universe Design tool, and use a reporting application such as Web Intelligence or Crystal Reports.

25.3 Visual Difference in the promotion management tool

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

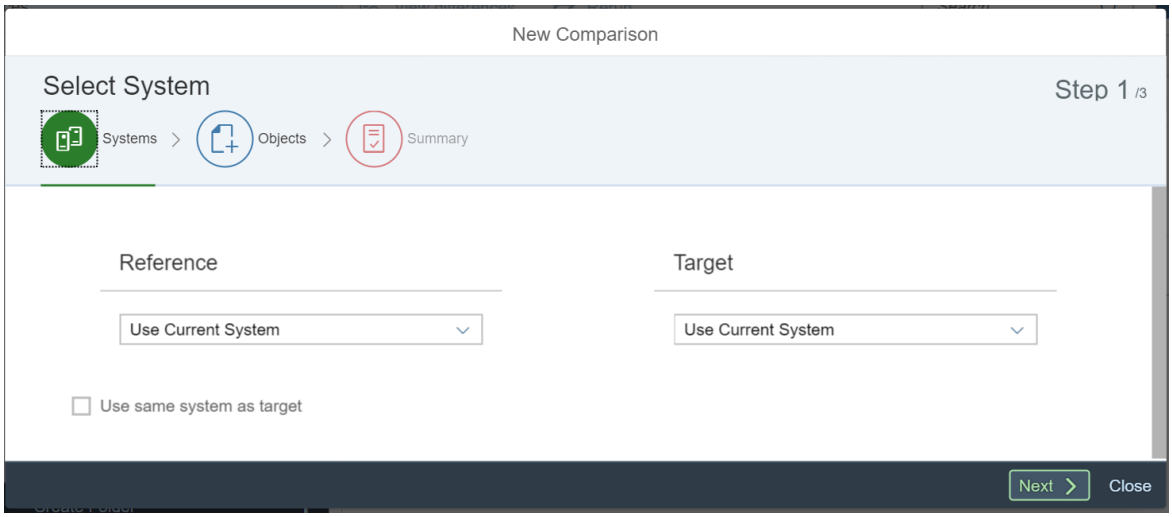
25.3.1 To compare objects or files using Visual Difference

To compare files using visual difference, complete the following steps:

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.

   > **i 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:

   > **i 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.

> **i 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.

25.3.2 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.

   > **i 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*.

25.3.3 To schedule the comparison

To schedule the comparison of files or objects, complete the following steps:

1. Click *Schedule*.
   The *Visual Difference -Schedule* window is displayed.
2. Select the frequency to schedule the comparison from the *Run Comparison* list.
3. Specify the number of retries allowed, and the retry interval in the respective fields.

   > **i** Note
   >
   > You can specify the retry interval only if you specify the number of retries.

4. Specify the report name, and click *Browse* to browse for the location in which you want to save the report.
   The *Save Job in* window is displayed.
5. Select the required folder where you want to save the report, and click *OK*.

   > **i** Note
   >
   > Depending on the option you select from the *Run Comparison* list, you must specify the date and time respectively for comparison.

6. Click *Schedule*.

   The user can view the comparison object or the difference report in the Visual Difference Viewer at a later point of time. The *Compared Differences* page is displayed with the list of folders and files or comparison reports.

   The Compared Difference page also contains the following options:

   - *History* This option allows you to view the history of comparison.
   - *Rerun* This option runs the comparison again.
   - *Schedule* This option allows you to schedule the comparison.

26 Auditing

26.1 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

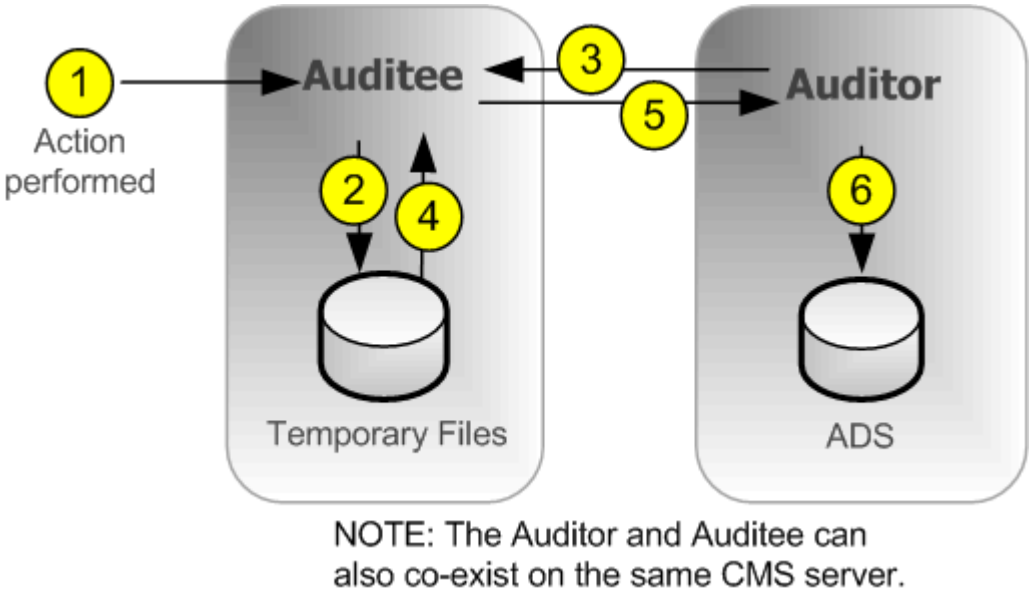
The Central Management Server (CMS) acts as the system auditor, while each server or application that triggers an auditable event acts as an auditee. When an audited event is triggered, the auditee will generate a record and store it in a local temporary file. At regular intervals, the CMS communicates 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

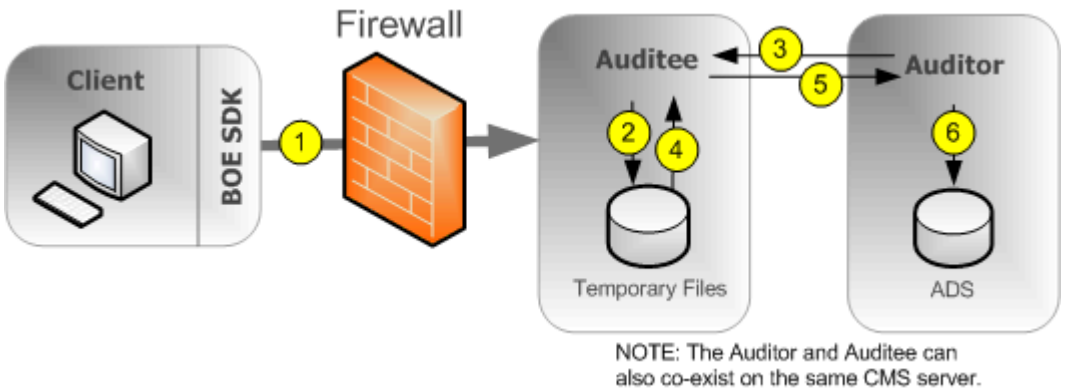
In cases of server generated events, the CMS can act as both Auditee and Auditor.



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.



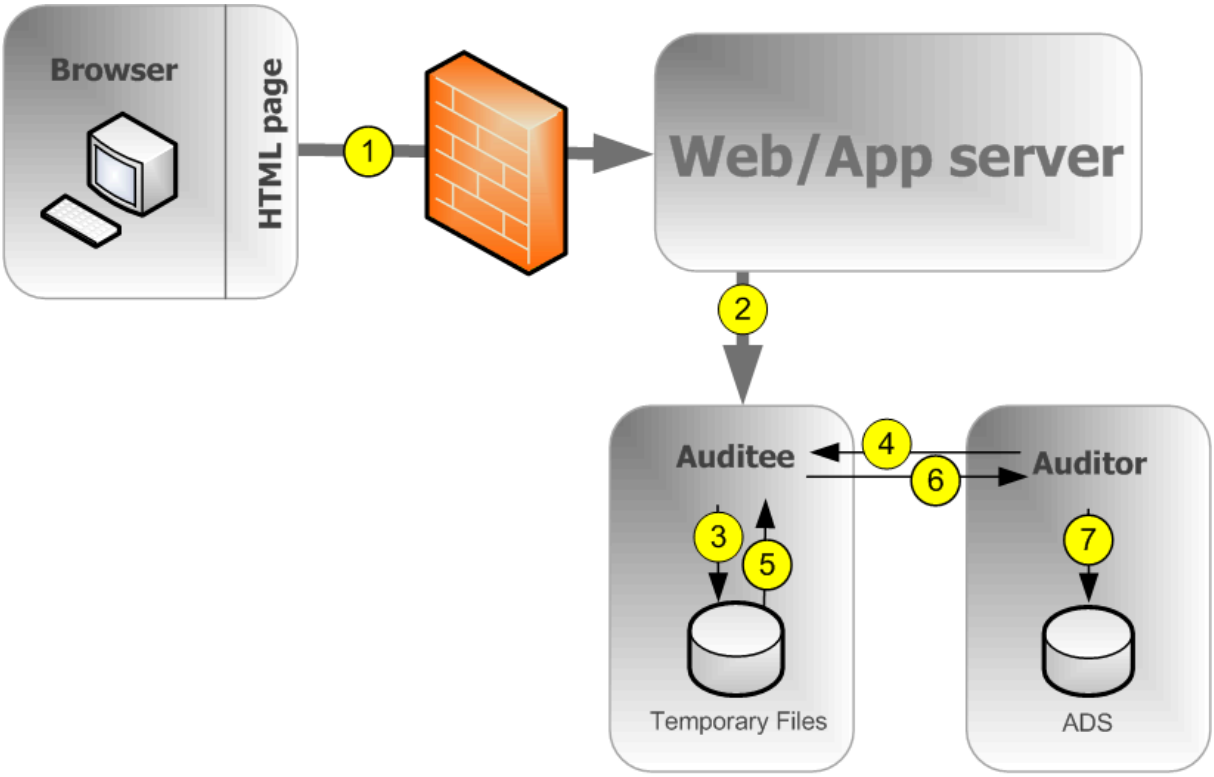
1. The client connects to the CMS, which will act as the auditee. The client provides its IP address and machine name, which the auditee then verifies.

> **i 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

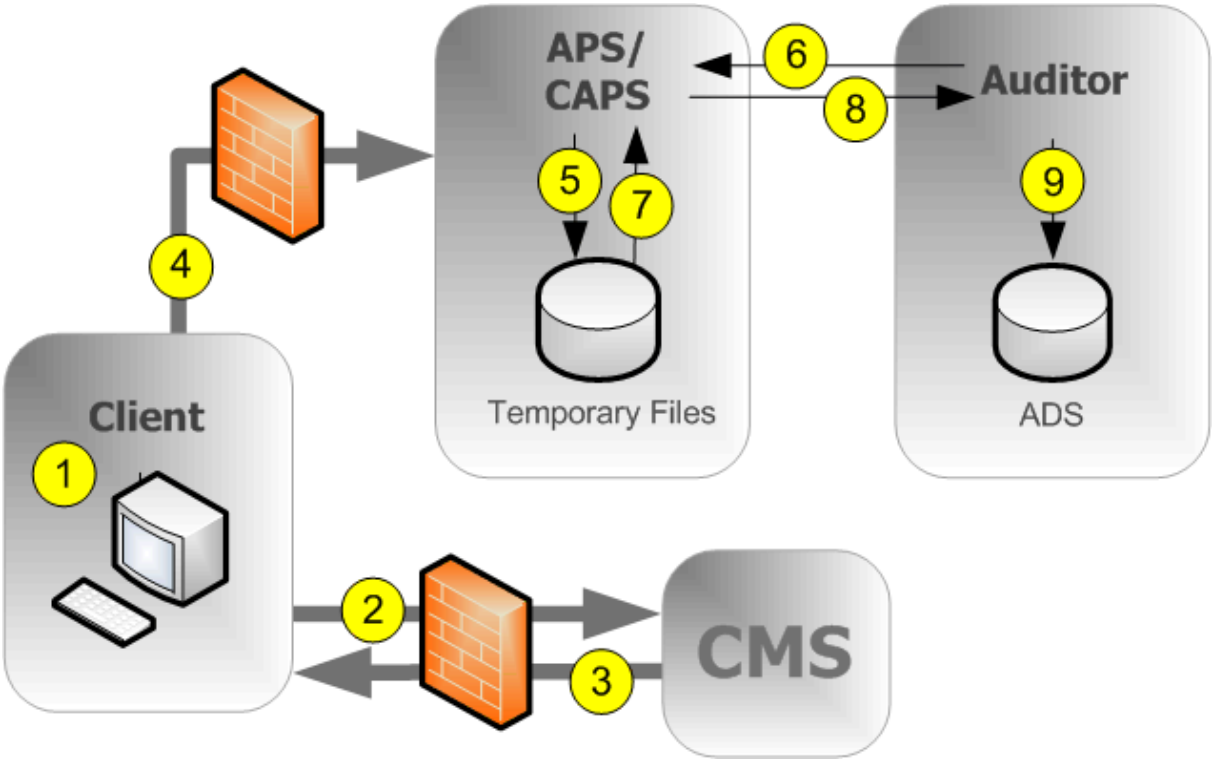
This includes online applications such as BI launch pad, Central Management Console, SAP BusinessObjects Web Intelligence, and so on.



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.



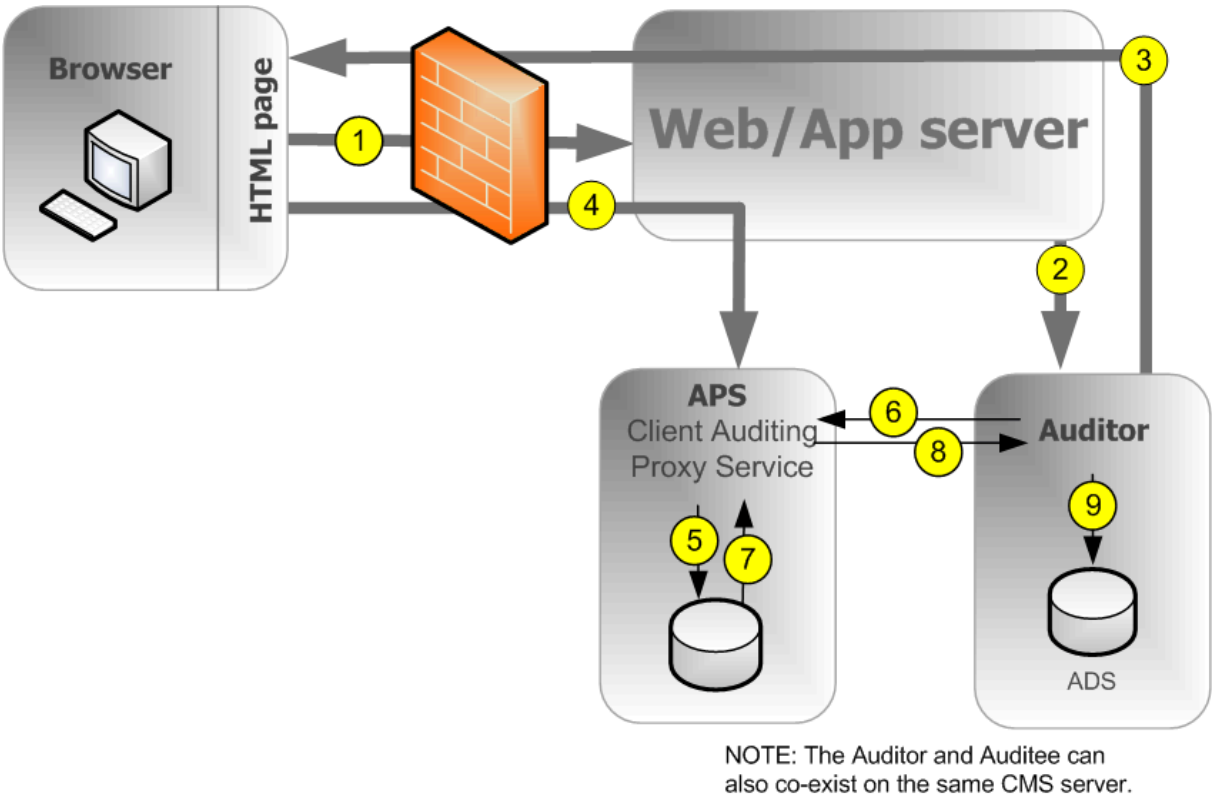
1. The user performs an operation that may be audited.
2. The client contacts the CMS to check if the operation is configured to be audited.
3. If the action is set to be audited, the CMS communicates this information to the client.
4. The client sends the event information to the Client Auditing Proxy 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.

   > **i** 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:

- Analysis edition for OLAP (AOLAP)
- BI Launch Pad (BILP)
- Business View Manager (BVM)
- Central Configuration Manager (CCM)
- Central Management Console (CMC)
- OpenDocument
- Information Design Tool (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- Translation Management Tool (TMT)
- Web Intelligence Rich Client (WIRC)
- Lumira Desktop Application (Discovery)
- Lumira Designer Application

> **i 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 493]

26.2 CMC Auditing page

The *Auditing* page in the CMC has the following areas:

- *Status Summary*
- *Set Events*
- *Set Event Details*
- *Configuration*

26.2.1 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.

> **i** 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.

Metric	Details
	• 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.
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.

26.2.2 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.*

26.2.2.1 To Configure Auditing Events

To configure the auditing events, perform the following steps:

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 • Drill Out of Scope. • Page Retrieved • Promotion Management Configuration • Rollback • VMS Add • VMS Retrieve • VMS Check-in • VMS Check-out

Auditing Level	Events captured
	• VMS Export • VMS Lock • VMS Unlock • VMS Delete • Cube Connection • MDAS Session **i Note** You can view more events when the add-ons are installed.
Custom	You select a custom set of events.

i 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.

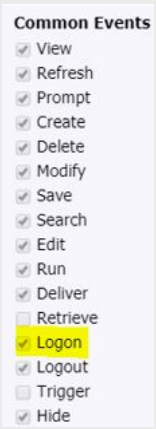
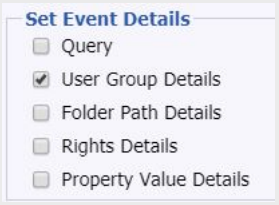
3. Select *Custom*, click the events you want to capture in the list below the *Set Events* slider.
4. Click the optional details under *Set Event Details* that you want to record with the events, recording fewer details increases system performance.

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)*
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.

26.2.2.2 Enhanced Event Detail Recording in Audit Detail Table

> **Note**
>
> - You should have sufficient knowledge regarding the CMC Auditing page [page 328], 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.

26.2.3 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.

> **i** 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.

26.2.3.1 To configure your Auditing Data Store database settings

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>`

Database type	Connection name
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.

   > ℹ 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.

   > ℹ 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.

27 Platform Search

27.1 Platform Search

The Platform Search application in the BI platform enables users to search content within the BI platform repository.

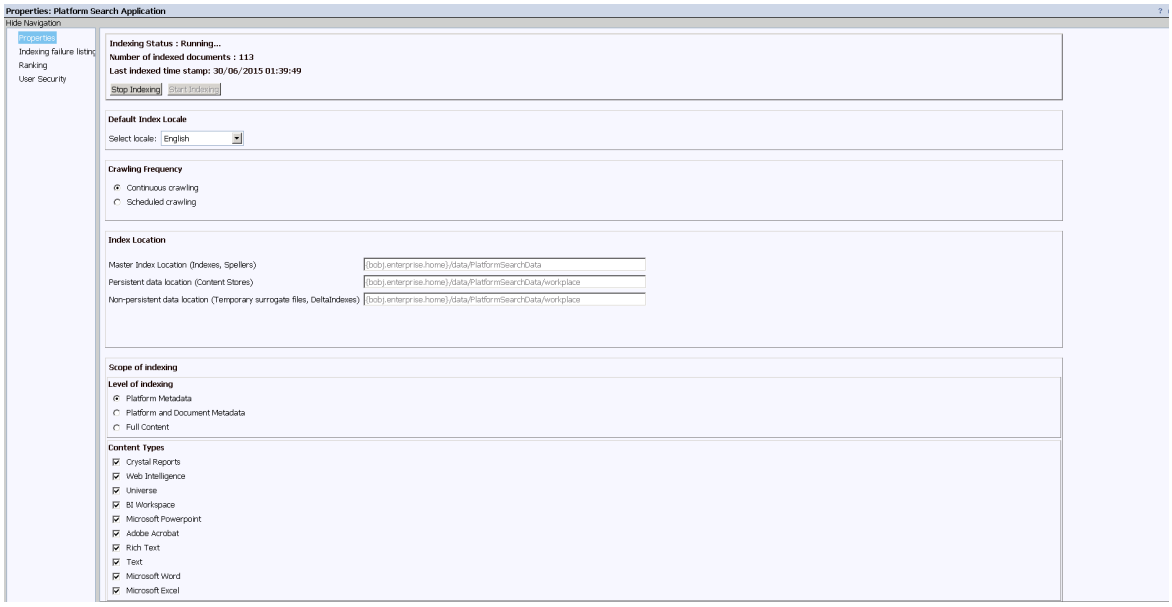
The Platform Search application can be accessed from the CMC home page to perform the following tasks:

- To set the application properties
- To view the indexing failure listing
- To set the user's security rights
- To schedule an object

27.1.1 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.
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*. **i 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. **i 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. **i 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 • Flash • Agnostic • Analytic • Hyperlink • Program • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset

Option	Description
	• VISI.Lums • VISILums • User • UserGroup

5. Click *Save & Close*.

> **i** 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.

27.1.2 Indexing Failure Listing

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 following steps:

1. Go to the *Applications* area of the CMC.
2. Select *Platform Search Application*.
3. Click *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.

27.1.3 Setting User Security Rights

You can manage security settings for Platform Search 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, and view or modify the rights that the principal has to an object.

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

An access control list specifies the users that are granted or denied rights on an object.

To assign a principal to an access control list, and to specify the rights that the principal has to the object, perform the following steps:

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*.
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.

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

27.1.3.2 To remove rights for a principal

1. Click *Manage* > *User Security*.
   The *User Security* dialog box appears and displays the access control list.
2. Select the object name for which you want to remove the rights.
3. Click the *Remove* tab.
   The *Access* right changes to *No Access*.

27.1.3.3 To view rights for a principal

Perform the following steps to view rights for a principal on an object.

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
Sort By Type
Sort By Right Name
From Access Level

- 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)
  Apply To (Select All, Object Only, Sub Objects Only, and Object and Sub Objects)

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

27.1.3.4 To modify security for a principal on an object

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. Advanced rights let you customize the rights for a principal on top of the access levels the principal already has. Complete the following steps to assign advanced rights to a principal on an object:

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*.
4. Click the *Advanced* tab.
5. Click *Add/Remove rights*.
6. Modify the rights for the principal.

27.1.3.5 To Reset Security Settings

Resetting security settings on an object removes all the explicit access levels or rights the object has, including the out of the box settings, if any. It retains only the inherited levels and rights.

1. Click the *Reset Security Settings* tab.
   The *Reset Security Settings: Platform Search Application* dialog box appears.
2. Select one or both of the following options:
   - Reset security settings on object Platform Search Application.
   - Reset security settings on all children and descendants of object Platform Search Application.

   > **i Note**
   >
   > In case you select both the options, a confirmatory dialog box appears. Click OK to proceed.
3. Click *Continue* to reset the security settings.

27.1.4 Scheduling an object

The scheduling options enable you to schedule an object in Platform Search.

To access the Schedule Options for the Platform Search application, complete the following steps:

1. Go to the *Folders* area of the CMC and click the *Platform Search Scheduling* folder.
2. Right click *Platform Search Scheduling object* and select *Schedule*.
3. Set the *Platform Search Schedule Duration* by specifying the Schedule Duration.
4. Click *Save* to save the schedule duration.
5. Click *Instance Title* to specify a title for the instance.
6. Click *Schedule*.
7. Click *Recurrence* and select a recurrence pattern from the *Run Object* drop-down menu.
   When you select a recurrence pattern, the application prompts you to provide additional information. The following table lists the additional information you must provide for each recurrence pattern:

Run Object Options	Additional Information Required
Now	None
Once	Define the Start and End date/time
Hourly	Define the Hour and Minute, and then define the Start and End date/time
Daily	Define the number of days, and then define the Start and End date/time
Weekly	Select the days of the week, and then define the Start and End date/time
Monthly	Define the number of months, and then define the Start and End date/time
Nth Day of month	Select the day of the month, and then define the Start and End date/time
1st Monday of Month	Define the Start and End date/time
Last Day of Month	Define the Start and End date/time
X Day of Nth Week of the Month	Select the week and the day, and then define the Start and End date/time
Calendar	Select a customized calendar, and define the start and end date/time.

8. Enter the number in the *Number of retries allowed* and the required time in the *Retry interval in seconds* fields.
9. Click *Schedule*.
10. Click *Schedule For* and specify for whom you want to schedule an object.
    - Select Schedule only for myself if you want to schedule for yourself and click *Schedule*.
    - Select Schedule for specified users and user groups to schedule for a specific set of users or user group. The *Available* section appears. Move the users and groups you want to add from the *Available users/groups* list to the *Selected users/groups* list and click *Schedule*.

> **i Note**
>
> You can schedule an object for a minimum duration of 1 minute to the maximum duration of 1 year or 525600 minutes. By default, Platform Search sets the schedule duration as 20 minutes.

28 Working with Federation

28.1 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, Flash, Word, text, rich text, and Shockwave Flash 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.

28.2 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.

28.3 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.

28.3.1 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 350]

28.3.2 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 350]

28.3.3 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. **i 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.

28.3.4 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.

28.3.5 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.

> **i** Note
>
> Default access levels are not replicated, but references are maintained.

28.4 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

28.4.1 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

28.4.2 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.

> **i** 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 372]

28.4.3 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.

> **i** 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.

> **i** 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.

> **i** 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.

28.5 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.

> ℹ 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.

> ℹ 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.

> ℹ 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*.

> ℹ 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.

28.6 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 in Universe Designer, 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”.

28.7 Managing remote connections

Remote connection objects contain the information needed to connect to a remote BI platform deployment.

> **i** 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.

28.7.1 Creating remote connections

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.

You can create folders and subfolders to organize your remote connections.

28.7.1.1 To create a remote connection folder

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.

28.7.1.2 To create a remote connection

To connect to a remote BI platform deployment, you must create a remote connection in Federation.

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`**
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.

Field	Description
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*.

28.7.2 Modifying remote connections

After you create a remote connection, you can modify its properties and security options.

To modify a remote connection:

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*.

28.8 Managing replication jobs

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.

> **i 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.

28.8.1 Creating replication jobs

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.

28.8.1.1 To create a replication job

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. **i 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.

Option	Description
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.
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. **i 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*.

28.8.2 To schedule a replication job

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.

28.8.3 Modifying replication jobs

After you create a replication job in Federation, you can modify its properties.

28.8.3.1 To modify a replication job

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.

28.8.4 Viewing a log after a replication job

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:

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`

28.9 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.

28.9.1 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.

> **i** 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.

28.10 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.

28.10.1 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.

> **i** 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.

> **i** 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.

28.10.2 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.

28.11 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.

28.11.1 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*.

28.11.2 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.

> ℹ 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*.

28.11.3 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*.

28.12 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.

28.12.1 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.

> **i** 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)".

> **i 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 349]

28.12.2 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".

> **i 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.

28.12.3 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.

> **i** 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 349]

28.13 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.

> **i** 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.

28.13.1 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.

> **i** Note
>
> The CUID may or may not be the same, depending on the import choices you select in the LifeCycle Manager.

28.13.2 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".

> **i** 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.

28.13.3 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.

   > **i** 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.

28.13.4 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.

28.14 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
```

> **i** 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.

> **i** 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 381]
Using Web Services in Federation [page 369]
Current release limitations [page 380]

28.14.1 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 364]

28.14.2 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"`.

   > **i 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) 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.

12) 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 377]
Current release limitations [page 380]

29 Managing Replication Lists

29.1 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. **i Note** All objects are supported, although not at the individual level.
Reports	Crystal reports, Web Intelligence documents, and Dashboards objects. **i 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.

i 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

29.1.1 Creating replication lists

Replication lists are located in the Replication Lists area of the CMC. You can organize replication lists in folders and subfolders that you create.

29.1.1.1 To create a replication list folder

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.

29.1.1.2 To create a replication list

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.

Dependency object options	Definition
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 supported dependencies for selected Flash objects	Replicates any Crystal reports, hyperlinks, Web Intelligence documents or universes that the Flash object depends on.
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*.

29.1.2 Modifying Replication Lists

After you create a replication list, you can modify its properties or objects.

29.1.2.1 To modify properties in a replication list

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 386]

29.1.2.2 To modify objects in a replication list

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 386]

30 Publications

30.1 Design tasks

30.1.1 Creating a publication in the CMC

1. Under *Folders* in the Central Management Console (CMC), navigate to the folder where you want to create a publication.
2. Right-click the selected folder, and select *New* > *Publication*.
   The *New Publication* dialog box appears with general property options displayed.

   > **i** Note
   >
   > The *Summary* tab shows brief information of a publication while creating a publication or viewing properties of a publication.

3. (Required) In the *Title* field, enter the title of the publication.
4. (Optional) In the *Description* field, enter a description of the publication.
5. (Optional) In the *Keywords* field, enter keywords that are associated with the publication's content.
6. In the *Source Documents*, click the *Add* button.
7. In the *Select Source Documents* dialog box, select one or more source documents to add to the publication.
8. Click *OK*.

   > **i** Note
   >
   > The *Refresh At Runtime* check box is selected by default for each source document. It refreshes the document against its data source when the publication runs.
   >
   > If you do not want to refresh a source document when the publication runs, clear the *Refresh At Runtime* check box for the document.

9. Click *Save & Close*.

30.1.2 Opening a Publication for Editing

1. Locate the publication in the Fiorified BI launch pad:
   a. In the *My Home* group, click the *Folders* tile, and navigate to the folder where you created the publication.
   b. Click the ••• icon beside the publication and select *Properties*.

The *Properties* page of the publication is displayed. Here, you can modify various properties of the publication and save the changes.

2. Locate the publication in the Central Management Console (CMC) in the BI platform:
   - Double-click the publication.
   - Right-click the publication and select *Properties*.

   The *Properties* page of the publication is displayed. Here, you can modify various properties of the publication and save the changes.

The publication opens in a new window.

30.1.3 Defining General Properties for a Publication

You define properties for a publication in the *Properties* page.

In CMC or Fiorified BI Launch pad:

1. Open the publication for which you want to define the general properties.
   The *Properties* page appears, displaying the publication's general properties and title.
2. (Optional) In the *Description* box, enter a description of the publication.
3. (Optional) In the *Keywords* box, enter keywords that are associated with the publication's content.
4. Click *Save & Close*.

30.1.4 Adding Source Documents

You can add, modify, and remove documents to a publication in the *New Publication* page at any given time while creating a publication.

When choosing source documents, the dynamic content document type determines which options are available.

1. In the *New Publication* page, expand *General*, and select *Source Documents*.
2. Click the + *(Add)* icon.
3. In the *Select Source Documents* dialog box, locate and select dynamic content documents of the same document type to include in the publication.
4. Click *OK*.

   The selected source documents appear in the *Items* list in the *New Publication* page. The check box in the *Refresh At Runtime* column is selected by default for all source documents. When this check box is selected, the document is refreshed against its data source when the publication runs. If you do not wish to do so, clear the check box for that document in the *Refresh At Runtime* column.

   > **i Note**
   >
   > To improve system performance, clear the check box in the *Refresh At Runtime* column for each document.

5. You can set the order in which documents appear, when sending source documents as an attachment or a merged PDF file. In the *New Publication* page, in the *Source Documents* area, select a document in the *Items* list, and click *Move Up* or *Move Down* icon to reorder the documents.
6. Click *Save and Close*.

30.1.4.1 Replacing third-party source documents

A third-party (also called "agnostic") source document does not originate in the BI launch pad. For example, it may be a Microsoft Word, Adobe PDF, or Microsoft Excel file.

Before you can replace a third-party source document, you must have Edit access rights for the document.

Although you cannot update the content of third-party documents, you can replace a third-party document with a more recent version of it. This enables you to view the latest source information in documents that originate outside of the launch pad.

1. Right-click a third-party document and select *Organize* > *Replace File*.

   If the *Replace File* menu option is unavailable for a third-party document, you do not have Edit rights for the document.
2. In the *Replace File* dialog box, click *Browse*, and select a more recent version of the source document file on your computer.

   If a message appears, stating that the file does not match the source document's file format, you have chosen a file in a different format than the original source document. Click *OK* to close the message, and then click *Browse*, and select the correct source document.
3. Click *Replace*.
4. In the confirmation message, click *OK* to update the third-party document.

30.1.5 Selecting Enterprise recipients

You select Enterprise recipients for a publication in the *Schedule* dialog box.

1. In the *Schedule* dialog box, click *Destinations* in the navigation list, and click *Enterprise Recipients*.
2. Choose recipients for the publication:
   a. Under *Available*, click *User List* to display a list of all users in the BI platform or *Group List* to display a list of all user groups in the BI platform.
   b. Select users or user groups, and move the users or groups to the *Selected* list.

   Enter a recipient's user name, full name, or email address in the *Find title* box to quickly locate the user in the *Available Recipients* list. To simultaneously select several users or user groups, hold down the `SHIFT` or `CTRL` key and click each user or group. To exclude recipients, select a user or user group in the *Selected* list, and move the user or group to the *Excluded* list.
3. Click *OK*.

30.1.6 Selecting dynamic recipients

Dynamic recipients are recipients who are not BI platform users. You select dynamic recipients for a publication in the *New Publication* dialog box.

Before you can specify dynamic recipients, you must have a dynamic recipient source designed and ready for use. The dynamic recipient source contains recipient data; it can be a Crystal report, a Web Intelligence document, or a custom-coded data provider. For information about creating a custom-coded dynamic recipient source, see the *SAP BusinessObjects Business Intelligence Platform Java SDK Developer Guide*.

Dynamic recipient data comes from the query and may not match data that appears when you view a document. Depending on how a query is built, dynamic recipient sources created in the Web Intelligence component may contain values that do not correspond to data in the publication's source documents. For example, a filter in a report may exclude relevant values, or duplicate records may appear because a query was set to retrieve duplicate rows. Review the full list of dynamic recipients during the publication design process.

To more efficiently process publications, use the *Recipient Identifier* list to sort recipient data by the recipient ID.

1. Open the publication to select dynamic recipients for.
2. In the *Properties* dialog box, click *Dynamic Recipients* in the navigation list.

   Crystal report dynamic recipient sources cannot be in `.rptr` format.
3. Under *Choose the source for the dynamic recipients*, select either *Web Intelligence Report Dynamic Recipient Provider* or *Crystal Reports Dynamic Recipient Provider*.
4. Locate and select the object to use as a dynamic recipient source, and click *OK*.
5. If you chose a Web Intelligence document as a dynamic recipient source, in the *Select the datasource name for the document* list, select a query that appears in the document.
6. In the *Recipient Identifier (required)* list, select a field that contains the recipient identity values.
7. (Optional) In the *Full Name* list, select a field that contains the full names of recipients.
8. If you intend to deliver the publication to email addresses, in the *Email* list, select a field that contains the recipient email addresses.
9. Decide which recipients in the dynamic recipient source to distribute the publication to:

   - To send the publication to all dynamic recipients, select the *Use entire list* check box.
   - To send the publication to particular dynamic recipients, clear the *Use entire list* check box, and then, under *Available*, select the check box for a recipient, and move the recipient to the *Selected* list.

   Enter a recipient's user name, full name, or email address in the *Find title* box to quickly locate the user in the *Available Recipients* list. To exclude a recipient, select the check box for the recipient, and move the recipient to the *Excluded* list.
10. Click *OK*.

After specifying dynamic recipients for the publication, you can personalize the publication for dynamic recipients. To do this, map a field in the source document to a column in the dynamic recipient source.

30.1.7 Selecting a Destination for a Publication

You select a destination for a publication while you create or schedule a publication.

1. In the *New Publication* or *Publication Schedule* page, expand *General*, and select *Destinations*.
2. (Optional) To avoid storing publication instances on your system, delete the *Default Enterprise Location* under *Selected Delivery Destinations* list.
3. Set a low instance limit on the publication object.

   For instructions, see the *SAP BusinessObjects Business Intelligence Platform User Guide*.
4. Click *Add* under *Select Delivery Destinations*, select the check box beside each destination that you want to send the publication to.

   If you want to create a shortcut to the publication, select both *BI Inbox* and *Default Enterprise Location* as destinations.

   If the publication will be sent to email recipients and you want to embed a link to the Enterprise location in the email body, select both *Email* and *Default Enterprise Location* as destinations.

   The destination you chose appears in the left navigation pane of the *Select Destinations* dialog.
5. If necessary, select a destination to configure from the left navigation pane.
   Options for the destination appear.
6. (Optional) To choose a name for the publication, select *Use specific name*, and enter a name or select a placeholder in the *Add Placeholder* list.

   If you do not choose a name, a system-generated name is assigned to a publication. When the publication runs, a value will be inserted in each placeholder.
7. (Optional) If you selected *Use specific name* and the publication contains multiple documents that you want to assign individual names to, select the *Specific Name per Document* check box, and enter a name or select a placeholder in the *Add Placeholder* list for each document.

   If you do not choose a name, the same system-generated name is assigned to each document.
8. (*Email* only) To embed a link to the Enterprise location in the email body, position the cursor in the *Message* box, and select *Viewer* in the *Add placeholder* list under the box.

   The placeholder *%SI_VIEWER_URL%* is inserted in the email body. It will be replaced by a link when the publication runs. If you are unable to embed a link, confirm that you selected both *Email* and *Default Enterprise Location* as the destination.
9. (*BI Inbox* only) Under *Send As*, click *Shortcut* to create a shortcut to the publication or *Copy* to create a copy of the publication.

   If you are unable to create a shortcut, confirm that you selected both *BI Inbox* and *Default Enterprise Location* as the destination.
10. If you selected multiple destinations, repeat steps 5 to 10 for each destination to select and configure the destination.
11. Click *Confirm*.

30.1.7.1 Scheduling destination options

Option	Description
Default Enterprise Location	Sends the object to the default enterprise location.
BI Inbox	Sends the object to the user's BI launchpad inbox.
Email	Sends the object to the user's email.
FTP Server	Sends the object to an FTP server location.
SFTP Server	Sends the object to an SFTP server location.

The *Deliver objects to each user* check box is selected by default for all destinations. However, in some cases, you may not want to deliver objects to each user. For example, three recipients have identical personalization values so they receive the same data in publication instances. If you clear the *Deliver objects to each user* check box, one publication instance is generated and delivered to all three recipients. If you select the *Deliver objects to each user* check box, the same publication instance is delivered three times (once for each recipient).

If you are sending the publication to the *FTP Server*, *SFTP Server*, or *File System* destination and some recipients share identical personalization values, you can clear the *Deliver objects to each user* check box to decrease overall processing time. When you clear *Deliver objects to each user*, placeholders used when configuring destinations will contain the publisher's (not the recipient's) information.

30.1.8 Selecting a Recurrence Pattern

The recurrence pattern determines how often a publication runs. You select a recurrence pattern for a publication in the *Schedule* dialog box.

1. Right-click the publication to set a recurrence pattern for and select *Schedule*.
2. In the *Schedule* dialog box, click *Recurrence*.
3. In the *Run object* list, select a recurrence pattern.
4. In the *Number of retries allowed* box, enter the number of times the server should attempt to rerun a failed job.
5. In the *Retry interval in seconds* box, enter how long the server should wait before attempting to rerun a job.
6. Click *Schedule*.

The publication runs at the scheduled times.

30.1.8.1 Recurrence pattern options

Option	Description
Now	Runs the object one time, starting immediately

Option	Description
Once	Runs the object once, at the specified start time. If you schedule an object with events, the object will run once, if the event is triggered between the start and end times. Select when to start and to stop running the object in the *Start Date/Time* and *End Date/Time* lists, and enter the date of the start and the stop times.
Hourly	Creates an instance every hour, at the specified time. The first instance will be created at the specified start time, and instances will be created hourly at that time, until the object stops running at the specified end time. Select the frequency at which to run the object in the *Hour(N)* and *Minute(X)* lists, select when to start and to stop running the object in the *Start Date/Time* and *End Date/Time* lists, and enter the date of the start and the stop times.
Daily	Runs the object once daily, at the specified start time. The first instance will be created at the specified start time, and instances will be created daily at that time, until the object stops running at the specified end time. Enter the interval at which to run the object in the *Days(N)* box, select when to start and to stop running the object in the *Start Date/Time* and *End Date/Time* lists, and enter the date of the start and the stop times.
Weekly	Runs the object each week on the selected days, at the specified start time. The first instance will be created at the specified start time, and instances will be created each week on those days at that time, until the object stops running at the specified end time. Select a check box for each day that you want to run the object, select when to start and to stop running the object in the *Start Date/Time* and *End Date/Time* lists, and enter the date of the start and the stop times.
Monthly	Runs the object on the specified date, at the specified start time, and at the specified monthly intervals. The first instance will be created at the specified start time, and instances will be created in monthly intervals at that time, until the object stops running at the specified end time. Select the interval at which to run the object in the *Month(N)* box, select when to start and to stop running the object in the *Start Date/Time* and *End Date/Time* lists, and enter the date of the start and the stop times.

Option	Description
Nth Day of Month	Creates an instance each month on the specified day, at the specified start time. The first instance will be created at the specified start time, and instances will be created on the specified day of each month at that time, until the object stops running at the specified end time. Enter the time to start and to stop running the object and the day of the month on which to run the object.
1st Monday of Month	Creates an instance on the first Monday of each month, at the specified start time. Enter the time to start and to stop running the object.
Last Day of Month	Creates an instance on the last day of each month, at the specified start time. Enter the time to start and to stop running the object.
X Day of Nth Week of the Month	Creates an instance each month on the specified day and week, at the specified start time. Enter the time to start and to stop running the object, the day of the week, and the week in the month to run the object.
Calendar	Creates an instance on each calendar date you specify, at the specified start time. Enter the time to start and to stop running the object, and select the calendar dates when you want to run the object.

30.1.9 Selecting Personalized placeholders for Publication Source Documents

You select personalized placeholders for a publication in the *Schedule* dialog box.

Before you can use personalized placeholders in publication instance names, the publication's source documents must use personalization to filter data.

When scheduling a publication instance, you can use placeholders in the *Use Specific Name* field for source documents, and you can combine text and placeholders—and use multiple placeholders—in a publication name.

1. Right-click the publication to select placeholders for and select *Schedule*.
2. In the *Schedule* dialog box, click *Destinations* in the navigation list.
3. Under *Show options for selected destinations*, select *Use Specific Name* and choose a placeholder for the publication name from the *Add placeholder* list.
   The placeholders you select appear in the *Specific Name* box for the document title.

4. To add individual documents:
   a. Under *Target Name*, select *Specific Name per Document*.
   b. For each document title, select a placeholder from the *Add placeholder* list.

   The placeholders you select appear in the *Specific Name* box for each document title.
5. Click *OK*.

After personalization is set up for a publication, personalized placeholders appear in the *Add placeholder* list in the *Destinations* dialog box.

30.1.10 Selecting Personalized Placeholders for Email Fields

You select personalized placeholders for a publication in the *Schedule* dialog box.

You can combine text and placeholders—and use multiple placeholders—in any email field. When scheduling a publication to an email destination, you can use placeholders in the *From*, *To*, *Cc*, *Bcc*, *Subject*, *Message*, and *Use Specific Name* fields.

1. Right-click the publication to select placeholders for and select *Schedule*.
2. In the *Schedule* dialog box , click *Destinations* in the navigation list.
3. In the *Destination* list, select *Email*.
4. Set the destination options, including placeholders, as needed.
5. Click *OK*.

30.1.11 Embedding Content from a Dynamic Source Document in an Email

You embed content from a source document for a publication in the *Schedule* dialog box.

You can embed content from dynamic content documents in the body of an email. For Crystal reports, you can embed content from a report. For Web Intelligence documents, you can embed an entire document or a single report tab.

1. Right-click the publication to take the content from and select *Schedule*.
2. In the *Schedule* dialog box, click *Formats* in the navigation list.
3. (Crystal reports only) Under *Format Options for Selected Document*, select the *mHTML* check box.
4. (Web Intelligence documents only) Choose whether to publish the entire document or one report tab:
   a. Under *Output Format*, select the *mHTML* check box.
   b. Under *Output Format Details*, select *All reports* to publish the entire document or *Select one report* and choose a report tab in the list.
5. Click *Destinations* in the navigation list.
6. In the *Destinations* dialog box, under *Select Destinations*, select the *Email* check box.

   The email configuration options appear.
7. In the *From* box, enter a name or email address or select *Email Address* in the *Add placeholder* list.

For example, you can enter **Robert**, **Publisher**, or **publisher@sap.com**. If you enter a name, the name is appended to your email server—for example, **Publisher@<EmailServer>**.

8. In the *Subject* box, enter a subject or select a placeholder.

   If you personalized the report, personalized placeholders are available in the *Add placeholder* list.
9. In the *Message* box, enter the message that you want to appear in the body of the mail.
10. To embed dynamic content in the *Message* box, position the cursor in the *Message* box where you want to embed content, and select *Report HTML Content* in the *Add placeholder* list.
    %SI_DOCUMENT_HTML_CONTENT% appears in the *Message* box. When the publication runs, the placeholder is replaced by personalized content from the dynamic content document.
11. If the publication contains other source documents, select the *Add Attachment* check box.

    Other source documents in the publication will be added to the email as attachments when the publication runs.
12. Click *OK*.

30.1.12 Adding a Publication Extension in the CMC

A publication extension is a library of code that applies business logic to publications. You must add a publication extension before you can use the extension in a publication.

Before you can use a publication extension, deploy the extension on all computers that run the Adaptive Processing Server, and then restart the Adaptive Processing Server and other servers that host a Publishing Service. The location of the server varies, depending on the operating system:

- In Windows, the server is located at `<InstallDir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\`
- In Unix, the server is located at `<InstallDir>/sap_bobj/enterprise_xi40/java/lib/`

You can add publication extensions only in the Central Management Console (CMC). (You cannot add them when designing a publication in the BI launch pad.)

To define the order in which to execute publication extensions, click *Move Up* or *Move Down* under the *Before Publication Delivery* list or the *After Publication Delivery* list. For more information about publication extensions, see the *SAP BusinessObjects Business Intelligence Platform Java SDK Developer Guide*.

1. In the CMC, go to the *Folders* management area, and locate the publication to add a publication extension to.
2. Right-click the publication and select *Properties*
3. In the *Properties* dialog box, expand *Additional Options* in the navigation list, and select *Publication Extension*.
4. In the *Publication Extension Name* box, enter a name for the extension.
5. In the *Class Name* box, enter the fully qualified class name for the extension.
6. (Optional) In the *Parameter* box, enter a parameter name.
7. To use the extension after processing but before delivery, above the *Before Publication Delivery* list, click the *Add* button.
   The extension is added to the *Before Publication Delivery* list.
8. To use the extension after delivery, above the *After Publication Delivery* list, click the *Add* button.
   The extension is added to the *After Publication Delivery* list.

9. Click *Save*.

30.1.13 Enabling Email Notification for a Publication Job in the CMC

Enable email notification when you want to receive an email message after a publication job runs.

Before enabling email notification, confirm that the Adaptive Job Server is properly configured.

You can enable email notification only in the Central Management Console (CMC). (You cannot enable it when designing a publication in the BI Launch pad.)

1. In the CMC, go to the *Folders* management area, and locate the publication job to enable email notification for.
2. Right-click the publication job and select *Schedule*.
3. In the *Schedule* dialog box, click *Notification* in the navigation list, and expand *Email Notification: Not in use*.
4. For successful publication jobs, to receive email notification at default recipient email addresses, select the *A job ran successfully* check box, and select *Use the Job Server's defaults* to use the default addresses on the Adaptive Job Server.
5. For successful publication jobs, to receive email notification at specified recipient mail addresses, select the *A job ran successfully* check box, select *Set the values to be used here*, and perform the following actions:
   a. In the *From* box, enter the email address or a name to send the notification from.
   b. In the *To* box, enter the email address of each recipient who should receive the notification.
   c. In the *Cc* box, enter the email address of each additional recipient who should be copied on the notification.
   d. In the *Subject* box, enter the subject of the notification.
   e. In the *Message* box, enter a message to accompany the notification.
6. For failed publication jobs, to receive email notification at default recipient email addresses, select the *A job failed to run* check box, and select *Use the Job Server's defaults* to use the default addresses on the Adaptive Job Server.
7. For failed publication jobs, to receive email notification at specified recipient mail addresses, select the *A job failed to run* check box, select *Set the values to be used here*, and perform the following actions:
   a. In the *From* box, enter the email address or a name to send the notification from.
   b. In the *To* box, enter the email address of each recipient who should receive the notification.
   c. In the *Cc* box, enter the email address of each additional recipient who should be copied on the notification.
   d. In the *Subject* box, enter the subject of the notification.
   e. In the *Message* box, enter a message to accompany the notification.
8. Click *Schedule*.

30.1.14 Enabling Auditing Notification for a Publication Job in the CMC

Enable audition notification when you want to audit successful or failed publication jobs.

You can enable auditing notification only in the Central Management Console (CMC). (You cannot enable it when designing a publication in the BI launch pad.) For more information about auditing, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

1. In the CMC, go to the *Folders* management area, and locate the publication job to enable auditing notification for.
2. Right-click the publication job and select *Schedule*.
3. In the *Schedule* dialog box, expand *Additional Options*, click *Notification*, and expand *Audit Notification: Not in use*.
4. To audit successful publication jobs, select *A job ran successfully*.
5. To audit failed publication jobs, select *A job failed to run*.
6. Click *Schedule*.

30.1.15 Selecting Events to Trigger a Publication

Event-based scheduling gives you additional control when a publication runs. Use events to trigger a publication to run or use a publication job to trigger an event.

For information about events, see the *SAP BusinessObjects Business Intelligence Platform User Guide*.

1. Click the *** icon beside the publication to select events for and select *Schedule*.
2. In the *Schedule* page, expand *General*, and select *Events* in the navigation list.
3. To specify file-based and custom events for a publication, click the *Events to wait for* field.
4. In the *Select Events* dialog, select the check box beside the events to move them to the *Selected Items* list and click *Add*.

   The events trigger the publication job to run.
5. To specify schedule events for a publication, click the *Events to trigger on completion* field.
6. In the *Select Events* dialog box, select the check box beside the events to move them to the *Selected Items* list and click *Add*.

   The events occur after the publication job runs.
7. Click *Schedule*.

30.1.16 Selecting a Server Group for a Publication

You cannot schedule publications across sites in a federation. For information about server groups, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

1. Click the *** icon beside the publication to select a server group for and select *Schedule*.
2. In the *Schedule* page, expand *General*, and select *Scheduling Server Group* in the navigation list.
3. To run the publication job at its site of origin, enable the *Run at origin site* toggle button.
4. Select a server group option, and click *Schedule*.

30.1.17 Selecting a Profile Resolution Method in the CMC

1. In the CMC, go to the *Folders* management area, and locate the publication to select a profile resolution method for.
2. Right-click the publication job and select *Properties*.
3. In the *Properties* dialog box, expand *Properties* option in the navigation list, and click *Advanced*.
4. Under *Profile Resolution Method*, perform either of the following actions:
   - Select *Do not merge* if you want profiles from multiple user groups to result in separate documents.
   - Select *Merge* if you want to apply profiles from multiple user groups to the same document.
5. Click *Save & Close*.

30.1.18 Selecting a Report Bursting Method in the CMC

1. In the CMC, go to the *Folders* management area, and locate the publication to select a profile resolution method for.
2. Right-click the publication job and select *Properties*.
3. In the *Properties* dialog box, expand *Properties* option in the navigation list, and click *Advanced*.
4. Under *Report Bursting Method*, select a report bursting method.
5. Click *Save & Close*.

30.2 Crystal report design tasks

30.2.1 Personalizing a Crystal Report Using Parameter Values

You personalize a Crystal report in the *Schedule* dialog box.

- Before you can use profiles to personalize data for Enterprise recipients, the profiles must be configured in the BI platform.
- Before you can perform this task, the Crystal report must contain parameters.

1. Right-click the Crystal report to personalize and select *Schedule*.
2. In the *Schedule* dialog box, click *Personalization* in the navigation list.
3. Review the parameter values under *Parameters* and note any values that need to be changed.
4. To change a default value, click the *Edit Values* button beside the default parameter value, select or enter the parameter value, and click *OK*.
5. Perform one of the following actions:
   - To override the default parameter personalization with Enterprise-recipient profile values, in the *Enterprise Recipient Mapping* column, select a profile in the list.
     If this profile is not configured in the BI platform, personalization will fail. If you need profiles added to the BI platform, contact your system administrator.
   - If you are using only default parameter values to personalize a report, select *Default value for all recipients* in the *Enterprise Recipient Mapping* column.

   The *Enterprise Recipient Mapping* column appears only if the publication is intended for Enterprise recipients.
6. To override the default parameter personalization with dynamic recipient personalization values, in the *Dynamic Recipient Mapping* column, select a dynamic recipient source in the list.

   The *Dynamic Recipient Mapping* column appears only if the publication is intended for dynamic recipients.

   If you are using default parameter values to personalize a report, select *Not Specified* in the *Dynamic Recipient Mapping* column.
7. Click *OK*.

30.2.2 Personalizing a Crystal Report by Filtering Fields

You personalize a Crystal report in the *Schedule* dialog box.

Before you can use profiles to personalize data for Enterprise recipients, the profiles must be configured in the BI platform.

When you use filters, a ViewTime selection formula is added to a report to filter data. The formula is applied when the publication runs and is not saved in the report. You can filter multiple fields in Crystal reports. Static-value profiles can filter only string fields in Crystal reports. To filter other types of fields, use expression profile values. If you map the incorrect type of field to the profile, personalization will fail.

This feature is not available for Crystal reports in `.rptr` format.

1. Right-click the Crystal report to personalize and select *Schedule*.
2. In the *Schedule* dialog box, click *Personalization* in the navigation list.
3. Under *Local Profiles*, in the *Report Field* column, select a Crystal report field in the list.

   The list of available fields includes all database fields and recurring formulas in the main report and in not-on-demand subreports.
4. In the *Enterprise Recipient Mapping* column, select a profile in the list.

   This profile maps the report to profile values defined for Enterprise recipients. If the profile is not configured in the BI platform, personalization will fail. If you need profiles added, contact your system administrator.

   The *Enterprise Recipient Mapping* column appears only for publications intended for Enterprise recipients.

5. In the *Dynamic Recipient Mapping* column, select a dynamic recipient source in the list.

   The report field is mapped to a column in the dynamic recipient source that contains corresponding values.

   The *Dynamic Recipient Mapping* column appears only for publications intended for dynamic recipients.
6. Repeat steps 2 to 5 for each report field you want to filter.
7. Click *OK*.

30.2.3 Selecting the Publication Format(s) for a Crystal report

You select the publication format for a Crystal report through *Publication Properties* > *Report Features* > *Formats*.

You can select and configure more than one publication format for a Crystal report. When you select a format, the available formatting options appear. For some options, such as *Crystal Reports* and *Crystal Reports (RPTR)*, no formatting options appear and the default source document formatting is applied.

1. Right-click the Crystal report to select a publication format, and select *Schedule*.
2. In the *Schedule* dialog box, click *Formats*.
3. Under *Format Options for Selected Document*, select a format to publish the Crystal report in.

   The options for the selected format appear.
4. Configure the formatting options as needed.
5. When the *Use the export options defined in the report* check box is available, perform one of the following actions:

   - Select the check box to use the default export options defined in the source document.
   - Clear the check box to configure export options for the format you selected, and then configure the options that appear.
6. Repeat steps 3 to 5 for each format in which you want to publish this Crystal report.
7. Click *OK*.

Repeat this task for each Crystal report in the publication.

30.2.3.1 Crystal Report Formatting Options

No additional options appear when you choose *Tab Separated Text (TTX)* as the formatting option. *PDF* options apply to source documents published as PDF files.

Microsoft Excel (97-2003)

Option	Description
Page Range	• To publish an entire report as an Excel file, select *All*. • To publish specific report pages, select *Pages*, enter the first page number in the *from* box, and enter the last page in the *to* box.
If you clear the *Use the export options defined in the report* check box, the following options are available:	
Set Column Width	• To define column widths relative to objects in a report, select *Column width based on objects in the*, and select an option in the list—*Whole report*, *Report Header*, *Page Header*, *Group Header #*, *Details*, *Group Footer #*, *Page Footer*, or *Report Footer*. • To define a constant width for all report columns, select *Constant column width (in points)*, and enter a number in the box.
Export page header and page footer	Select this check box to choose how frequently headers and footers appear in Excel files, and select an option in the list—*None*, *Once Per Report*, or *On Each Page*.
Create page breaks for each page	Select this check box to create page breaks that reflect the page breaks in a report.
Convert date values to strings	Select this check box to convert date values to text strings.
Show gridlines	Select this check box to include grid lines in Excel files.

Microsoft Excel (97-2003) (Data Only)

If you clear the *Use the export options defined in the report* check box, the following options are available:

Option	Description
Set Column Width	• To define column widths relative to objects in a report, select *Column width based on objects in the*, and select an option in the list—*Whole report*, *Report Header*, *Page Header*, *Group Header #*, *Details*, *Group Footer #*, *Page Footer*, or *Report Footer*. • To define a constant width for all report columns, select *Constant column width (in points)*, and enter a number in the box.
Export object formatting	Select this check box to preserve object formatting from a report.
Export images	Select this check box to publish report images in Excel files.
Use worksheet functions for summaries	Select this check box to use report summaries to create worksheet functions for Excel files.
Maintain relative object position	Select this check box to preserve the relative position of report objects.
Maintain column alignment	Select this check box to preserve the column alignment from a report.
Export page header and page footer	Select this check box to choose how frequently headers and footers appear in Excel files, and select an option in the list—*None*, *Once Per Report*, or *On Each Page*.
Simplify page headers	Select this check box to simplify page headers in a report.
Show group outlines	Select this check box to show group outlines from a report.

Microsoft Excel Workbook Data-only

If you clear the *Use the export options defined in the report* check box, the following options are available:

Option	Description
Set Column Width	• To define column widths relative to objects in a report, select *Column width based on objects in the*, and select an option in the list—*Whole report*, *Report Header*, *Page Header*, *Group Header #*, *Details*, *Group Footer #*, *Page Footer*, or *Report Footer*. • To define a constant width for all report columns, select *Constant column width (in points)*, and enter a number in the box.
Export object formatting	Select this check box to preserve object formatting in a report.
Export images	Select this check box to publish report images in Excel files.
Use worksheet functions for summaries	Select this check box to use report summaries to create worksheet functions for Excel files.
Maintain relative object position	Select this check box to preserve the relative position of report objects.
Maintain column alignment	Select this check box to preserve the column alignment from a report.
Export page header and page footer	Select this check box to choose how frequently headers and footers appear in Excel files, and select an option in the list—*None*, *Once Per Report*, or *On Each Page*.
Simplify page headers	Select this check box to simplify page headers in a report.
Show group outlines	Select this check box to show group outlines from a report.

Microsoft Word (97-2003)

Option	Description
Page Range	• To publish an entire report as a Word file, select *All*. • To publish specific report pages, select *Pages*, enter the first page number in the *from* box, and enter the last page in the *to* box.

PDF

Option	Description
Page Range	• To publish an entire report as a PDF file, select *All*. • To publish specific report pages, select *Pages*, enter the first page number in the *from* box, and enter the last page in the *to* box.
If you clear the *Use the export options defined in the report* check box, the following option is available:	
Create bookmarks from group tree	Select this check box to create bookmarks in the generated PDF file based on group tree.

Rich Text Format (RTF)

Option	Description
Page Range	• To publish an entire report as an RTF file, select *All*. • To publish specific report pages, select *Pages*, enter the first page number in the *from* box, and enter the last page in the *to* box.

Microsoft Word - Editable (RTF)

Option	Description
Page Range	• To publish an entire report as a Word file, select *All*. • To publish specific report pages, select *Pages*, enter the first page number in the *from* box, and enter the last page in the *to* box.
If you clear the *Use the export options defined in the report* check box, the following option is available:	
Insert page break after each report page	Select this check box to create page breaks that reflect the page breaks in a report.

Plain Text

If you clear the *Use the export options defined in the report* check box, the following option is available:

Option	Description
Number of Characters per Inch	Enter the number of characters that should appear per inch in a plain text file. The recommended range is between 8 and 16.

Paginated Text

If you clear the *Use the export options defined in the report* check box, the following options are available:

Option	Description
Number of Lines per Page	Enter the number of lines that should appear on each page of a paginated text file.
Number of Characters per Inch	Enter the number of characters that should appear per inch in a paginated text file. The recommended range is between 8 and 16.

Separated Values (CSV)

If you clear the *Use the export options defined in the report* check box, the following options are available:

Option	Description
Delimiter	Enter the character to use as a delimiter.
Separator	Enter the character to use to separate values, or select the Tab check box to separate values with tabs.
Mode	Select *Standard Mode* (the default) or *Legacy Mode*. In standard mode, you can control how report pages and group headers and footers appear in CSV output.
Report and page sections	• To export report and page sections, select *Export*. • If you do not want to export report or page sections, select *Do not export*. • To isolate report and page sections, select the *Isolate report/page sections* check box.

Option	Description
Group sections	• To export group sections, select *Export*. • If you do not want to export group sections, select *Do not export*. • To isolate group sections, select the *Isolate report/page sections* check box.

XML

If you clear the *Use the export options defined in the report* check box, the following option is available:

Option	Description
XML Exporting Formats	To specify the XML format, select an option in the list.

30.2.4 (Optional) Selecting Print Options for a Crystal Report in a Publication

You can select print options for a Crystal report in *Publication Properties* > *Report Features* > *Print Settings*.

Before you can set print options for the default printer:

- The printer must be installed and configured properly.
- The Crystal Reports Job Server must be running on an account that has sufficient privileges to access the printer you specify.
  For more information, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

You can print instances in Crystal reports format each time a publication runs, using the Crystal Reports Job Server's default printer or a different printer. The BI platform prints instances after the publication is personalized but before delivery.

1. Right-click the Crystal report to set print options, and select *Schedule*.
2. In the *Schedule* dialog box, click *Print Settings*.
3. Under *Documents*, select the Crystal report that you want to print when the publication runs.
4. Select the *Print Crystal reports when scheduling* check box.
   The Crystal report print options appear.
5. Select *Default printer* to print to the Job Server's default printer, or select *Specify the printer* and select the printer's path and name:
   - If the job server runs on Windows, in the *Specify the printer* box, enter `\\<PrintServer>\<PrinterName>`
     Replace `<PrintServer>` with the name of your printer server and `<PrinterName>` with the name of your printer.

- If the job server runs on Unix, confirm that the Unix is shown (not hidden), and enter the print command that you usually use in the *Specify a printer* box.
  For example, enter `lp -d <PrinterName>`

6. In the *Number of Copies* box, enter the number of copies to print.
7. Under *Page Range*, select *All* to print all pages in the publication or *Pages* and enter the page range to print.
8. (Optional) In the *Set collate option to* list, select *Collate*, *Do not collate*, or *Use printer defaults*.
9. (Optional) In the *Page Scaling* list, select *Scale to fit*, *Only shrink to fit*, or *Do not scale*.
10. (Optional) To center report content on the page, select the *Center the page* check box.
11. (Optional) If the Crystal report is wide and you want it to print on one page, select the *Fit horizontal pages into one page* check box.
12. Click *Schedule*.

30.2.5 (Optional) Selecting a Recipient Delivery Rule for a Crystal Report in Publication

Recipient delivery rules determine whether a publication is delivered to a particular recipient after processing and personalization. After creating a publication, you can open the publication and change the delivery rules for it.

1. Click the *** icon beside the publication to set delivery rule for and select *Properties*.
2. In the *Publication Properties* window, expand *Report Features*, and click *Delivery Rules* in the navigation list.
3. Under *Recipient Delivery Rule*, select *Deliver individual document when condition is met* or *Deliver all documents only when all conditions are met*.
4. In the *Condition* column beside each document, select the condition to be met before the publication is delivered.
5. Click *Save and Close*.

30.2.6 (Optional) Selecting a Global Delivery Rule for a Publication

Global delivery rules determine whether a publication can be processed and delivered to all recipients. You can set a global delivery rule on any Publication in the BI Platform based on Crystal reports.

1. Click the *** icon beside the publication to set delivery rule for and select *Properties*.
2. In the *Publication Properties* page, expand *Report Features*, and click *Delivery Rules* in the navigation list.
3. Under *Global Delivery Rule*, click *Browse*.
   The *Select Document* dialog box appears, you can select a Crystal report as source of the global delivery rule.

> **i Note**
>
> The Crystal report must contain an alert.

4. Locate and select the Crystal report, and click *OK*.
5. In the *Condition* list, select the applicable condition for the publication to be processed and delivered.
6. Click *Save and Close*.

30.2.7 (Optional) Formatting a merged PDF file from Crystal reports

Before you can format a merged PDF file:

- Crystal reports must have titles in order to be included in a merged PDF file. To set the title for a report, open the report in SAP Crystal Reports, select *File* > *Summary Info*, and enter a title for the report in the *Title* box on the *Summary* tab. Save the report and re-export it to the repository.
- In the Fiorified BI Launch pad, for a publication, in the *Properties* page, under *Source Documents*, the Crystal reports and PDF files that you want to merge must appear in the correct order.
- In the Fiorified BI Launch pad, for a publication, in the *Properties* page, expand *Report Features*.
- Under *Formats*, the *PDF* check box must be selected as a format for each Crystal report that you want to include in the merged PDF file.
- In the Fiorified BI Launch pad, in the *Schedule* page, under *Destinations*, the *Merge Exported PDF* check box must be selected for each destination that you want to send the merged PDF file to.

Ensure that the merged PDF contain detailed bookmarks that allow easier navigation. For each Crystal report listed,

- Select the report in the *Documents* list in the *Formats* area.
- Clear the *Use the export options defined in the report* check box.
- Select the *Create bookmarks from group tree* check box.

To format a merged PDF file, perform the following steps:

1. Click the *** icon beside the Publication to format a merged PDF file for and select *Properties*.
2. In the *Properties* page, expand *Report Features*, and click *Merged PDF Options* in the navigation list.
3. Create a table of contents for the merged PDF file:
   a. Enable the *Create Table of Contents* toggle button.
      The format options for the table of contents appear.
   b. In the *Title* box, enter a title for the table of contents.
   c. In the *Title Font* list, select the font, font size (in points), and font color for the title of the table of contents.
   d. In the *Item Font* list, select the font, font size (in points), and font color for items in the table of contents.
4. Set the page number format for the merged PDF file:
   a. Enable the *Apply Running Page Numbers* toggle button.
      The format options for page numbers appear.
   b. In the *Number Format* box, enter a format for page numbers.

      By default, the format is set to `Page &p of &P`. You can change the format, but you must use `&p` as a placeholder for the current page number and `&P` as a placeholder for the total number of pages.

c. In the *Number Location* list, select the page number orientation for the merged PDF file.
d. In the *Number Font* list, select the font, font size (in points), and font color for the page numbers.
e. If you want the table of contents to have page numbers, select the *Apply page numbers to Table of Contents pages* check box.

5. Set recipient logon credentials and permissions for recipient actions:
   a. Enable the *Set Restrictions* toggle button.
   b. In the *User Password* box, enter the password that recipients must enter to view the merged PDF file.
   c. In the *Owner Password* box, enter the password that recipients must enter to edit the merged PDF file.
   d. To allow recipients to print the PDF file, select the *Allow Printing* check box.
   e. To allow recipients to modify the PDF file, select the *Allow Modification of Contents* check box.
   f. To allow recipients to copy and paste PDF contents, select the *Allow Copy and Paste (Required for Embedded Flash Objects to Run)* check box.
   g. To allow recipients to modify annotations in the PDF file, select the *Allow Modification of Annotations* check box.
6. Click *Save*.

30.2.8 Configuring Database Logon Information for a Crystal Report in Publication

You can configure the database logon information that recipients use to log on to the database and refresh the data in the Crystal report.

Confirm that database settings for the Crystal report are correct or modify a report's default database setting. In the CMC, select *Folders*, select the Crystal report, and select *Manage* > *Default Settings* > *Database Configuration* to check the database information or to enter new information.

> **i Note**
>
> To avoid breaking existing schedule or publication, changes in CMC **Database Configuration** will only show up the next time you schedule or publish that Crystal report.

1. Click the *** icon beside the publication to configure database logon information for and select *Schedule* or *Properties*.
2. In the *Schedule* or *Properties* page, expand *Report Features*, and click *Database Logon* in the navigation list.
3. In the *Data Sources* list, select a data source.
   The database information for the data source appears in the *Details* section.
4. Confirm that the information in the *Database Server* field and the *Database* field is correct.
5. In the *User* field, enter the user name that recipients must use to log on.
6. In the *Password* field, enter the password that recipients must use to log on.
7. Click *Schedule* (or *Save* in *Properties* page).
   You can also modify the data source information that a Crystal report references in the report itself.
   Open the Crystal report in SAP Crystal Reports, select *Database* > *Set Datasource Location*. Select a connection, or create a new connection in the *Set Datasource Location* dialog box.

30.3 Web Intelligence document design tasks

30.3.1 Selecting the Publication Format for a Web Intelligence Document

You must select a publication format for each dynamic content source Web Intelligence document in a publication.

1. Right-click the Web Intelligence document to specify a publication format for and select *Schedule*.
2. In the *Schedule* dialog box, click *Formats* in the navigation list.
3. Under *Output Format*, select the check box beside the format to publish the Web Intelligence document in:
   - *Web Intelligence*
   - *Microsoft Excel*
   - *Adobe Acrobat*
   - *mHTML*
4. If you selected *Comma Separated Values (CSV)*, under *Format Options and Settings*, perform the following actions:
   a. In the *Text qualifier* list, select a text qualifier.
   b. In the *Column delimiter* list, select a column delimiter.
   c. In the *Charset* list, select the character set.
   d. If you want to enter a new character set, select the *Enter a new charset* check box, and enter the character set in the box.
   e. If you want to use the settings configured as the default, select the *Set as default values* check box.
   f. If you want to generate a comma-separated value for each data source, select the *Generate separate CSV per Data Provider* check box.
5. Repeat steps 3 to 4 for each format in which to publish the document.
6. Click *OK*.

30.3.2 Personalizing a Web Intelligence Document with a Global Profile Target

You can personalize a Web Intelligence document for Enterprise recipients by filtering with a global profile target.

- Before you can use a profile to personalize data for Enterprise recipients, the profile must be configured in the BI platform. If a profile is not configured in the platform, personalization will fail.
- Before personalizing a Web Intelligence document, ensure that the profile has a global profile target.

When you define personalization under *Global Profiles*, you do not need to set personalization options under *Filters*. If you need profiles added to the BI platform, contact your system administrator.

1. Right-click the Web Intelligence document to personalize and select *Schedule*.
2. In the *Schedule* dialog box, click *Personalization* in the navigation list.

3. Under *Global Profiles*, in the *Enterprise Recipient Mapping* column, select a profile in the list.

   This profile maps the document to the universe field (global profile target) that is filtered for Enterprise recipients.
4. Click *OK*.

30.3.3 Personalizing a Web Intelligence Document by Filtering Fields

Before you can use a profile to personalize data, the profile must be configured in the BI platform. If a profile is not configured in the platform, personalization will fail.

Static-value profiles can filter only string fields in source documents. To filter other types of fields, use expression profile values. If you map an incorrect type of field to the profile, personalization will fail. If you need profiles added to the platform, contact your system administrator.

Scheduling and publishing a Web Intelligence document to `.wid` format generates a `.wid` file. Filters in `.wid` files can be removed by any recipient with appropriate security rights. When the `.wid` file will be sent to recipients or destinations, use filters carefully. For example, if you filter a Web Intelligence document to limit the information that recipients can see and then send the published `.wid` file to recipients, any recipient with security rights to edit the document can remove or update the filter and access data that should not be visible.

1. Right-click the Web Intelligence document to personalize and select *Schedule*.
2. In the *Schedule* dialog box, click *Personalization* in the navigation list.
3. Under *Local Profiles*, for each profile listed in the *Title* column, select a profile from the list in the *Report Field* column.

   This profile maps the report field to profile values for Enterprise recipients.
4. Under *Local Profiles*, in the *Enterprise Recipient Mapping* column, select a profile the list.

   This profile maps the document to the universe field (global profile target) that is filtered for Enterprise recipients.
5. In the *Dynamic Recipient Mapping* column, select a profile in the list.

   The field in the source document is mapped to the column that contains corresponding values in the dynamic recipient source.
6. Repeat steps 3 to 5 for each field to filter.
7. Click *OK*.

30.3.4 Editing Parameter (prompt) Values for an Object

If you don't want to use the default parameter (prompt) values in a content object, you can edit the values.

Parameters (prompts) ask you to enter information. In report objects, the information you enter can determine which data appears in a report. For example, in a report used by sales, a parameter can ask you to choose a region. When a region is selected, the report displays the results only for that selected region.

1. In the *Documents* tile, click the *** icon beside the object to edit parameter (prompt) values for and select *Schedule*.

2. In the *Schedule* page, expand *Report Features*, and click *Prompts* in the navigation list.

   The parameter (prompt) options can differ from object to object depending on how your system administrator has configured the parameter or prompt. For example, program objects can appear in an *Argument* box.

   If the *Prompts* option is not available, the content object does not contain parameters or prompts.
3. (Crystal reports only) In the *Prompts* area, click *Edit Values...*, and edit a parameter value.
4. (Web Intelligence documents based on SAP BEx query only) In the *Prompts* area, click *Modify* to edit a prompt value or *Clear* to remove the value.

   In Web Intelligence documents, parameters are called as prompts. When a scheduled document runs, based on SAP Business Explorer (SAP BEx) queries, a prompt's value can be fixed or obtained by an SAP Business Warehouse (SAP BW) data source variable. Prompts can contain mandatory variables in SAP BW data sources.

   The SAP BW data source must be able to process the value provided for a prompt. If the data source cannot process a value, document execution fails. For example, SAP BW exit or customer exit variables are often used as dynamic variables in prompts.

   If the *Clear* button is not available, your administrator can enable it by setting `bex.dynamic_variable.schedule=true` in the `<InstallDir>\<WebAppServer>\webapps\boe\web-inf\config\custom\AnalyticalReporting.properties` file. For instructions, see the *Business Intelligence Platform Administrator Guide*.
5. Click *Schedule*.

30.4 Post-design tasks

30.4.1 Testing a Publication

Use the test mode in the BI Launch pad to send a publication to yourself before sending it to recipients.

When you're testing a publication and have added yourself as the recipient, the same information that is planned to be delivered to the recipients configured in the publication, is sent to you. If necessary, you can exclude selected recipients from the original group of recipients in test mode. This allows you to check how the publication content appears to your recipients.

1. Go to the folder where you've created the publication and select ••• (*Click here for more options*) → *Test Mode*.
2. (Optional) In the *Test Mode*, modify the recipients as required:
   a. Under *Enterprise Recipients*, click on Select.
   b. Under *Available Recipients*, include or exclude the users or user groups.
   c. Select *OK*.
3. (Optional) Under *Dynamic Recipients*, you can modify the recipient list that is retrieved from the document or you can remove the document.

4. Select *Test*.

The publication runs in test mode and once done, the publication is sent to the intended test recipients.

30.4.2 Scheduling a Publication to Run

When scheduling a publication, you can use the default recurrence pattern or enter new values, and you can change the recipients each time you schedule a publication.

To create a publication in the Fiorified Business Intelligence Launch pad, please refer to *Creating a Publication in the Fiorified BI Launch pad* section in the *Fiorified BI Launch pad User Guide*.

A publication can then be designed and saved before it can be scheduled to run.

1. Click the *** icon beside the publication to schedule and select *Schedule*.
2. In the *Schedule* page, expand *General*, and select *Recurrence* in the navigation list and confirm that the option selected in the *Run Report* list is correct.
3. Click *Schedule*.

30.4.2.1 Publication results - how to view

Publication results can be viewed by the publisher, by recipients, or in a log file for the publication job.

Viewing results as a publisher

You can view the results of a publication in various ways. After a publication runs, the publication history appears, listing publication instances, the times when the publication ran, and whether the publication succeeded or failed. In the *Instance Time* column, you can click a link to a publication instance to view instances generated for all recipients when the publication ran.

Viewing log files for publication jobs

Log files are useful for troubleshooting a publication and for identifying which recipients did not receive a publication instance. The BI platform logs publication job information as each batch of personalized publication instances is processed and then consolidates the details into one or more log files. The maximum log file size is 10 MB and is non-configurable. If you run a high-volume publication with many details, the publication instance may have several log files.

You can view log files for a publication instance in the following ways in the *History* dialog box:

- To view the last log file in a series, in the *Status* column, click the status (Success, Failed, or Running), and click *View Log File* at the bottom of the *Instance Details* dialog box. You can view the last log file while a publication is running.

- To view all log files, in the *Instance Time* column, click the link for a publication instance. Log files are listed after the personalized instances.

Log files are updated with new information every two minutes. If a publication job has been running less than two minutes, the log file may have a status of Pending.

Viewing results as a recipient

The following table summarizes the ways you can view a publication:

Destination	How to view the publication result
Default Enterprise Location	Dynamic recipients cannot log on to the BI platform to view publication results. As a recipient, you can view only your own personalized publication instances in the platform. You cannot view publication instances that are personalized for other recipients.
BI Inbox	Dynamic recipients cannot log on to the BI launch pad to view publication results.
Email	Log on to your email to view embedded publication content or to download the attachment or attachments.
FTP server	Log on to your FTP host.
SFTP server	Log on to your SFTP host.
Local disk	Go to the location specified when the publication was designed.

30.4.3 Subscribing or Unsubscribing from a Publication

To subscribe to a publication after it is scheduled, subscribe to its recurring instance or reschedule the publication.

You must have appropriate access rights to a publication before you can subscribe to it.

Only Enterprise recipients can subscribe to or unsubscribe from a publication. Dynamic recipients cannot subscribe to or unsubscribe from publications.

1. On the home page, click the *Folders* tile.
2. Navigate to the folder where you have a publication for which you want to subscribe to or unsubscribe from.
3. Click the *** icon beside the publication and select *Subscribe* or *Unsubscribe*.

   You are now either subscribed or unsubscribed from a publication based on your selection.

30.4.4 Subscribing or Unsubscribing from a Publication Instance

After a recurring publication is scheduled, Enterprise recipients can subscribe to its first recurring instance. For example, when a publication is scheduled to run twice a week, you can subscribe to the first publication instance, but not the second one.

You must have appropriate access rights to a publication before you can subscribe to its instances.

Only Enterprise recipients can subscribe to or unsubscribe from a publication instance. Dynamic recipients cannot subscribe to or unsubscribe from publication instances.

1. In the *My Home* group, click the *Folders* tile.
2. Navigate to the folder where you have a publication and its instance for which you want to subscribe to or unsubscribe from.
3. Click the *** icon beside the publication and select *History*.
4. In the *History* page, click the *** icon beside the instance and select *Subscribe* or *Unsubscribe*.

   You are now either subscribed or unsubscribed from a publication instance based on your selection.

30.4.5 Redistributing a Publication Instance

When you want to resend an instance to a recipient but do not want to rerun an entire publication, you can redistribute successful publication instances to all or some of the original recipients.

Only recipients specified when the publication was originally run can receive redistributed instances.

1. Perform one of the following actions:
   - In the BI launch pad, right-click a publication and select *History*.
   - In the Central Management Console (CMC), right-click a publication and select *Actions* > *History*.
2. In the *History* dialog box, select a successful publication instance.
3. Perform one of the following actions:
   - In the launch pad, select *More Actions* > *Reschedule*.
   - In the CMC, select *Actions* > *Reschedule*.
4. Choose which recipients will receive redistributed instances:
   - To redistribute an instance to Enterprise recipients, click *Enterprise Recipients*, and click the > button to move recipients from the *Available* list to the *Selected* list.
   - To redistribute an instance to dynamic recipients:

   a. Click *Dynamic Recipients*, and confirm that columns mapped to recipient IDs, full names, and email addresses are correct.
   b. To redistribute the publication to all dynamic recipients, select *Use entire list*.
   c. To redistribute the publication to selected dynamic recipients, click the > button to move recipients from the *Available* list to the *Selected* list.

5. Click *Redistribute*.
   The publication history appears, and the redistributed instance has a status of Running. The date in the *Instance Time* column is updated to reflect the redistribution time.

30.4.6 Retrying a Failed Publication

Before retrying a failed publication, view the log file for the publication instance, address any errors, and reschedule the publication.

Using the option to “Retry” failed instances of a publication, you can:

- Overwrite the "failed" instance (*Run Now* and *Reschedule* create new instances, but *Retry* uses the failed instance itself).
- Process only the failed recipients, in case of a partial failure.
- Run the full job without creating a new instance, in case of a complete failure.

> **i Note**
>
> You can also perform auto-retry by specifying the *Number of retries allowed* and the *Retry interval in seconds* under the *Recurrence* property of the publication. In case of a failure, it attempts to run the publication again.

1. Select the failed publication instance.
2. Perform either of the following actions:
   - In the BI Launch pad, select *More Actions* > *History*.
   - In the Central Management Console (CMC), select *Actions* > *History*.
3. Right-click on the failed instance and click *Retry*.
   The instance status changes to *Running*. Wait till the status changes to *Success*.

If the publication fails again, review the new log file and fix any errors that occurred.

31 Rights Appendix

31.1 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*.

31.2 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) **i 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.

31.2.1 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

For more information on *General Rights*, refer to General rights [page 420].

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

31.3 Rights for specific object types

31.3.1 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).

31.3.2 Categories

The rights in this section are general rights that have a specific meaning in the context of public and personal categories.

> **i** 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.

31.3.3 Crystal reports

The rights in this section apply to Crystal reports only.

> **i** 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.

31.3.4 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.

31.3.5 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.

> **i** Note
>
> Users and subgroups can inherit rights from group membership.

> **i** 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.

31.3.6 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.

31.3.7 Universe (.unv) rights

The rights in this section apply to universes created with the universe design tool, or .unv 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.

> **i** Note
>
> Universe rights apply only when you import universes from the CMS in the universe design tool application. These rights do not apply when the universe is saved to local disk.

Right	Description
Add objects to the folder	Lets you add restriction sets or objects to the universe. To do this, you also require the *Edit Access Restrictions* right.
View objects	Lets you access and view the universe.
Edit objects	This right lets you do the following: • Edit the universe in the CMC or in the universe design tool. • Lock or unlock the universe. To unlock a universe, you also require the *Unlock Universe* right.

Right	Description
Delete objects	Lets you delete the universe.
Translate objects	Lets you to save translated universe object names using the translation management tool. **Note** You can also save translations if you have the *Edit objects* right explicitly granted as long as the *Translate objects* right is not explicitly denied.
New List of Values	This right lets you do the following: • Associate new lists of values with objects. • Edit existing lists of values. **Note** This right does not prevent you from creating cascading lists of values.
Print Universe	Lets you print the universe.
Show Table or Object Values	Lets you see the values associated with tables or objects in the universe.
Edit Access Restrictions	Lets you edit access restrictions (overloads) for the universe.
Unlock Universe	Lets you do the following: • Unlock the universe if it is locked by another user. • Export the universe from the CMS. To unlock a universe, you also require the *Edit objects* right.
Data Access	Lets you retrieve data from the universe and refresh documents based on the universe. To do this, you also require this right on the universe design tool application, the document, and the universe connection.
Create and Edit Query based on the universe	Lets you create documents and edit queries that are based on the universe.

31.3.8 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. **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.

31.3.9 Universe object-access levels

When designers create a universe using the universe design tool, or 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.

> **i** Note
>
> Object-access level security settings override any security settings that the universe inherits.

> **i** 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 431]

31.3.9.1 Assigning universe object-access levels

To set universe object-access level security, you require the *Modify the rights users have to objects* right on the universe.

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.

31.3.10 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. **Note** This right applies to .unv universes only.
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.
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.

31.3.11 Applications

31.3.11.1 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

31.3.11.2 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

Right	Description
Send to FTP location	Enables a user to send objects to an FTP location
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.

31.3.11.2.1 Rights for collaboration applications

These access rights apply to SAP Jam, when the application is configured in the BI platform.

Right	Description
Comment on documents owned by the user	Enables a user to comment on documents and instances that the user owns
View comments on documents owned by the user	Enables a user to view comments on documents and instances that the user owns
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 application.

31.3.11.3 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)

Right	Description
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.

31.3.11.4 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.
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.

Right	Description
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).

31.3.11.5 Strategy Builder

These access rights apply to Strategy Builder and can affect goals management in Performance Manager or specific features in Strategy Builder.

Right	Description
Create, Modify, or Delete Goals	Enables a user to add, edit, or remove goals in Performance Manager
View Goals	Enables a user to see goals in analytics
Access to Goal Management	Enables a user to view goals on the *Goals Management* page in Performance Manager
Publish Goals	Enables a user to publish goals in Performance Manager
Access to Strategy Builder	Enables a user to access the Strategy Builder in Performance Manager
Create, Modify, or Delete Roles	Enables a user to administer the roles used to publish goals and metrics for particular audiences in Strategy Builder
Create, Modify, or Delete Strategies	Enables a user to create strategies that link roles and that publish goals and metrics in Strategy Builder
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object

Right	Description
	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.

31.3.11.6 Universe design tool

Right	Description
Check Universe Integrity	Enables a user to check universe integrity
Refresh Structure Window	Enables a user to refresh the structure window
Use Table Browser	Enables a user to view database data, using the table browser
Apply Universe Constraints	Enables a user to apply predefined universe constraints to users of an imported universe
Link Universe	Enables a user to link two universes and share components
Create, Modify or Delete Connections	Enables a user to create, modify, and delete universe connections that are stored in the BI platform repository or stored as personal or shared connections
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.

31.3.11.7 Information design tool

Right	Description
Administer security profiles	Enables a user to open the security editor

Right	Description
	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.

31.3.11.8 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
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

Right	Description
	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.

31.3.11.9 SAP BusinessObjects Mobile

Right	Description
Log on to SAP BusinessObjects Mobile application	Enables a user to log on to the BI platform from the Mobile application and to view documents
Subscribe to document alerts	Enables a user to subscribe to document and recurring-instance alerts If a user has been granted this right in the past (even if it is no longer granted), the user can still receive subscribed alerts. Users must explicitly unsubscribe to an alert if they do not want to receive it. To subscribe to document alerts and recurring instances for schedules, a user must have "Full Control" access to the `System Events` folder, under *Events* in the CMC.
Save documents to device's localstore	Enables a user to save documents on a mobile device If a user has been granted the "Save documents locally on the device" right in the past (even if it is no longer granted) and has saved documents on the mobile device, the documents still exist on the device, but they are not synchronized during the synchronization process.
Send documents from device as an email	Enables a user to send reports in an email message

Right	Description
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.

For more information, see the *SAP BusinessObjects Mobile Installation and Deployment Guide*.

31.3.11.10 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

32 Server Properties Appendix

32.1 About the server properties appendix

This server properties appendix lists and describes properties that can be set for each BI platform server.

32.1.1 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. **i 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`**.

32.1.2 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
- Web Application Container 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. **i 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. **i 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. **i 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. **i 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. **i 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

Web Application Container Server properties

General properties

Property	Description	Default Value
Service Startup Timeout (seconds)	How long the WACS will wait for its hosted services to start before it times out. If the timeout passes, the WACS will not provide services that haven't started yet. On a slower machine, you can consider specifying a larger value. If you specify a value that is too small, and the WACS doesn't start before timing out, restore the default settings of the WACS through the Central Configuration Manager (CCM).	1200

TraceLog Service properties

Property	Description	Default Value
Log level	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. Use for debugging only. CPU usage may increase, impacting performance). The available menu choices are: • *Unspecified* • *None* • *Low* • *Medium* • *High*	Unspecified

Business Process BI Service properties

Property	Description	Default value
No configuration properties		

Query Builder Service properties

Property	Description	Default value
No configuration properties		

RESTful Web Service - System Property Configuration properties

Property	Description	Default Value
Show Error Stack	When enabled, the error log includes RESTful web service error messages for debugging purposes. It should not be used otherwise, or when there is a security concern where details of the BI platform are revealed.	Not selected
Default Number of Objects on One Page	The number of entries that will be listed per page. Developers can override this setting with the &pageSize=<m> parameter in the RESTful Web Services SDK.	50
Enterprise Session Token Timeout (minutes)	The expiry time a logon token will remain valid. Beyond this time, a new login token must be generated.	60
Session Pool Size	This is the number of cached sessions to be stored at one time that is used to improve server performance. 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 (minutes)	The time in minutes that cached sessions will expire.	2
Enable HTTP Basic Authentication	If this setting is not enabled, RESTful web service requests must use a logon token. When this setting is enabled, users must provide their name and password the first time they make a RESTful web service request. When enabled, the *Default Authentication Scheme for HTTP Basic* drop down menu appears.	Not selected
Default Authentication Scheme for HTTP Basic	When *Enable HTTP Basic Authentication* is checked, one of four authentication types may be selected. Note that names and passwords are transmitted in clear text unless HTTPS options are used. Accepted values are: • *secEnterprise* • *secDAP* • *SAPR3* • *secWinAD*	Blank. However, if *Enable HTTP Basic Authentication* is selected, defaults to *secEnterprise*.

RESTful Web Service - Cross-Origin Resource Sharing Configuration properties

Property	Description	Default Value
Allow Origins	This setting is to permit users with CORS-capable browsers access to java-scripted pages that must access multiple domain names. Add each domain name and separate each by a comma. For example, http://origin1.server.com:8080, http://origin2.server.com:8080. By default, browsers are allowed access to all domains (*).	* (an asterisk)
Max Age(minutes)	This is the maximum time that browsers may cache HTTP requests.	1440

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**

BOE Web Application Service properties

Property Type	Description	Default Value
Authentication Type	The authentication type that is used to authenticate users logging on to BI launch pad. Accepted values are: • *AD Kerberos* • *AD Kerberos SSO* • *Enterprise* • *LDAP*	*Enterprise*
Default AD Domain	The default Active Directory domain is used so that users do not have to supply a domain when they log in. For example, if the default domain is set to "mydomain" and a user logs on with the username "user", the Active Directory logon authority tries to authenticate "user@mydomain.com".	Blank
Service Principal Name	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	Blank

Property Type	Description	Default Value
Keytab File	The full path to a keytab file. A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	Blank

Web Services SDK and QaaWS properties

Property	Description	Default Value
Enable Kerberos Active Directory Single Sign On	Whether to enable Kerberos AD Single Sign-on for Web Services SDK and QaaWS.	**FALSE**
Default AD Domain	The default Active Directory domain is used so that users do not have to supply a domain when they log in.	Blank
Service Principal Name	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	Blank
Keytab File	The full path to a keytab file. A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	Blank

HTTP configuration properties

Property	Description	Default Value
Bind to All IP Addresses	Whether to bind to all network interfaces or not. If your server has more than one NIC, and you want to bind to a specific network interface, uncheck this property.	**TRUE**
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTP service is provided. You can only specify a value if you uncheck *Bind to All IP Addresses*.	**`localhost`**
HTTP Port	The port on which HTTP service is provided.	6405 The range of allowed values is 1 to 65535.
Maximum HTTP Header Size	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

Configuration of HTTP through proxy properties

Property	Description	Default Value
Enable HTTP through Proxy	Whether to enable the HTTP through Proxy connector on the WACS. This is typically checked in deployments with a reverse proxy.	**FALSE**
Bind to All IP Addresses	Whether to bind the HTTP through proxy port to all network interfaces or not.	**TRUE**
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTP through Proxy service is provided. You can only specify a value if you uncheck *Bind to All IP Addresses*.	**`localhost`**
HTTP Port	The port on which HTTP service in a reverse proxy deployment is provided. You can only specify a value if you check *Enable HTTP through Proxy*.	6406 The range of allowed values is 1 to 65535.

Property	Description	Default Value
Proxy Hostname	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can only specify a value if you check *Enable HTTP through Proxy*.	Blank
Proxy Port	The port of your forward or reverse proxy server. You can only specify a value if you check *Enable HTTP through Proxy*.	0 The range of allowed values is 1 to 65535.
Maximum HTTP Header Size	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

HTTPS configuration properties

Property	Description	Default Value
Enable HTTPS	Whether to enable HTTPS/SSL communication.	**FALSE**
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTPS service is provided. You can only specify a value if you check *Enable HTTPS*.	`localhost`
HTTPS Port	The port on which HTTPS service is provided. You can only specify a value if you check *Enable HTTPS*.	443 The range of allowed values is 1 to 65535.
Proxy Hostname	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can only specify a value if you check *Enable HTTPS*.	Blank
Proxy Port	The port of your forward or reverse proxy server. You can only specify a value if you check *Enable HTTPS*.	0 The allowed range of values is 1 to 65535.
Protocol	The encryption protocol to use. You can only specify a value if you check *Enable HTTPS*.	TLS Allowed values are TLS or SSL.
Certificate Store Type	The type of certificate store that contains your certificates and private keys. In most cases, this will be *PCKS12*. You can only specify a value if you check *Enable HTTPS*.	PKCS12 Allowed values are PKCS12 or JKS.
Certificate Store File Location	The full path to the certificate file. You can only specify a value if you check *Enable HTTPS*.	Blank
Private Key Access Password	PKCS12 certificate stores and JKS keystores have private keys that are password protected, to prevent unauthorized access or theft. Enter the password that you specified when you generated the certificate store here, so that WACS can access private keys from the certificate store. You can only specify a value if you check *Enable HTTPS*.	Blank

Property	Description	Default Value
Certificate Alias	The alias of the certificate inside the certificate store. If this is not specified, and a certificate store that contains more than one certificate is used, the first certificate in the store is used. In most cases, you do not need to specify a value. You can only specify a value if you check *Enable HTTPS*.	Blank
Enable Client Authentication	If client authentication is enabled, only clients that have keys stored in the Certificate Trust List file are can get WACS services. Other clients are rejected. You can only enable client authentication if you check *Enable HTTPS*.	**FALSE**
Certificate Trust List File Location	The full path to the certificate trust list file. You can only specify a value if you check *Enable HTTPS* and *Enable Client Authentication*.	Blank
Certificate Trust List Private Key Access Password	The password that protects access to the private keys in the Certificate Trust List file. You can only specify a value if you check *Enable HTTPS* and *Enable Client Authentication*.	Blank
Maximum HTTP Header Size	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

Concurrency properties (per connector)

Property	Description	Default Value
Maximum Concurrent Requests	The number of concurrent HTTP or HTTPS requests that each connector (HTTP, HTTP through Proxy, or HTTPS) can process simultaneously.	**150** The range of allowed values is 1 to 1000.

Active directory configuration properties

Property	Description	Default Value
Krb5.ini File Location	The full path to a `krb5.ini` file that stores Kerberos configuration properties.	Blank
bscLogin.conf File Location	The full path to a `bscLogin.conf` file.	Blank

32.1.3 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.		
Connection Pooling	Either enables or disables the connection pool. Possible values are: • Enabled - With Timeout • Enabled - Without Timeout • Disabled **i 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). **i 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`

Property	Description	Default Value
Enable HTTP Chunking	Either enables or disables the HTTP chunking. **i 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. **i 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. **i 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.		

Property	Description	Default Value
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. **i 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
Network Layer	Specifies the network layer used by the connection. **i 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. **i 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.

Property	Description	Default Value
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 441]

32.1.4 Crystal Reports Services Properties

The Crystal Reports service category includes the following servers:

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Crystal Reports 2020 Report Application Server Properties
- Crystal Reports 2020 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.

> **i 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. **i 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. **i 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.

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. **i 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.

i 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. **i 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. **i 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. **i 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. **i 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 2020 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 2020 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. **i 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 2020 Processing Server Properties

i Note

When you modify any of these properties, you must restart the server for the changes to take effect.

Crystal Reports 2020 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. **i 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. **i 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. **i 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. **i Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultDataDir%/CrystalReports2020ProcessingServer/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.

32.1.5 Analysis Services Properties

The Analysis services category includes the Adaptive Processing Server:

Multi-Dimensional Analysis Service Properties

Property	Description	Default Value
Maximum Client Sessions	Specifies the maximum number of MDAS sessions that can simultaneously be open on the server. When the number of open sessions reaches this number, any additional attempts to start MDAS sessions result in a "server unavailable" error message. You can change this value to optimize MDAS performance, depending on your needs and available hardware, but increasing the value may result in performance issues for both the MDAS and the database. The default value of 15 sessions is a conservative estimate. For installations where user queries are small, you can increase this value significantly, whereas installations where user queries are large would require a lower value.	The default value is set to 15. The valid range is 1 to 100.
Maximum number of cells returned by a query	Specifies the number of cells that are returned to a user in a single query. The user is prevented from executing a query that returns an extremely large number of cells, consuming a large amount of memory. If the user's query exceeds this cell limit, the user receives an error message.	The default value is 100000 cells.
Maximum number of members returned when filtering	Specifies the number of members retrieved when filtering by member. A very large number of retrieved members can consume a large amount of memory.	The default value is 100000 members.

BEx Web Applications Service Properties

Property	Description	Default Value
Maximum Client Sessions	The maximum number of client sessions allowed on the service.	The default value is 15 sessions.
SAP BW Master System	The name of the OLAP connection to the BW system that you created in the BI platform.	The default value is SAP_BW.
JCo Server RFC Destination	The name of the JCo Server RFS Destination that you entered in the BW system.	By default, this value is empty.
JCo Server Gateway Host	The name of the JCo Server Gateway Host that you defined in the BW system.	By default, this value is empty.
JCo Server Gateway Service	The name of the JCo Server Gateway Service that you defined in the BW system.	By default, this value is empty.
JCo Server Connection Count	Specifies the number of automatically created programs that can be used to handle calls from ABAP to Java for the service.	The default value is 3 connections.

32.1.6 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.

32.1.7 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.

Property	Description	Default Value
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. **i 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. **i 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**
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

Property	Description	Default Value
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
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. **i 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.

Property	Description	Default Value
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
Enable Current Activity Logs	Specifies whether complete traces are generated in the server's log files. **i 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

Property	Description	Default Value
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
Maximum Character Stream Size (MB)	Specifies the maximum character stream size sent to the Web Intelligence client. **i 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. **i 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 473]

32.1.7.1 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.

33 Server Metrics Appendix

33.1 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

> **i Note**
>
> For information about SAP BusinessObjects Explorer server properties and metrics, see the *SAP BusinessObjects Explorer Administrator's Guide*.

33.1.1 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 or Web Application Container Servers (WACS).
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 or Web Application Container Servers (WACS).
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 or Web Application Container Servers (WACS).
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 or Web Application Container Servers (WACS).
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 or Web Application Container Servers (WACS).

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.

Metric	Description
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.
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. **i 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.

33.1.2 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.

Metric	Description
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.
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.

Metric	Description
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.
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.

33.1.3 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)* **i Note** For more information about connection pools, refer to the *Data Access Guide*.

33.1.4 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.

33.1.5 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.

33.1.6 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.

Multi-Dimensional Analysis Service metrics

Metric	Description
Session Count	The current number of connections from MDAS clients to the server.
Cube Count	The number of data sources that are being used to supply data to the connections that have not timed out.
Query Count	The number of data requests that are open between MDAS clients and the server.

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.

Metric	Description
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.
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.

Metric	Description
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.
Number of Trended Metrics	The total number of metrics currently being recorded into the monitoring database.

BEx Web Applications Service metrics

Metric	Description
Session Count	A count of the total number of sessions active within a BEx Web Applications Service.

33.1.7 Web Application Container Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Web Application Container Servers.

> **Note**
>
> Web Application Container Servers also have all of the metrics that are described under the Adaptive Processing Server Metrics section.

Web Application Container Server Metrics

Metric	Description
List of Running WACS Connectors	A list of all running connectors on the server. If you do not see all of the connectors (HTTP, HTTPS and HTTP through proxy), it indicates either that the connector is not enabled or that it failed during startup
WACS Connector(s) Failed at Startup	Whether there are any failed connectors. If true, at least one connector failed to start. If false, all connectors are running. Do not run a server when one or more connectors has failed to start; you must troubleshoot the server to ensure that all connectors start properly.

Related Information

Adaptive Processing Server Metrics [page 482]

33.1.8 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.
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.

Metric	Description
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*.

33.1.9 Crystal Reports Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports Processing and Crystal Reports 2020 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.
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.

Metric	Description
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.
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.

Metric	Description
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 2020 Report Application Servers.

Crystal Reports 2020 Report Application Server Metrics

Metric	Description
metric_currentdoccount **i 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 **i 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_currentagentthreadcount **i 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 **i 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.

33.1.10 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.
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).

Metric	Description
Total number of threads	The total number of threads that have been created since the server was started (asynchronism threadpool).

34 Server Placeholders

34.1 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.

> **i 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.

> **i 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.
%DLLPRELOAD32%	The name of the LD_PRELOAD environment variable on 32-bit AIX systems.	On AIX, *LDR_PRELOAD*. This placeholder is an empty string on other machines.
%DLLPRELOAD64%	The name of the LD_PRELOAD environment variable on 64-bit AIX systems.	On AIX, *LDR_PRELOAD64*. This placeholder is an empty string on other 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>`.

Placeholder	Description	Default values
%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.	$LD_PRELOAD_ONCE$
%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.

Placeholder	Description	Default values
%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.
%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`.

Placeholder	Description	Default values
%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`.
%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\jre\bin`. On UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/jre/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/`.

Placeholder	Description	Default values
%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.
%PAGESERVER_EXE%	The name of the executable for the Crystal Reports 2020 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.

Placeholder	Description	Default values
%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`.
%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.	$LD_PRELOAD_ONCE$
%XCCACHE_EXE%	The name of the executable for the Dashboards Cache Server.	On Windows, `xccache.exe`. On UNIX. `boe_xccached`.
%XCPROC_EXE%	The name of the executable for the Dashboards Processing Server.	On Windows, `xcproc.exe`. On UNIX, `boe_xcprocd`.

Related Information

To view and edit the placeholders for a node [page 155]

35 Managing Cryptography Keys

35.1 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 502]
To create a new cryptographic key [page 504]
To delete a cryptographic key from the system [page 504]
To revoke a cryptographic key [page 505]
To view objects associated with a cryptographic key [page 503]
To mark cryptographic keys as compromised [page 505]

35.1.1 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.

Status	Description
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.

35.1.2 To view objects associated with a cryptographic key

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.

35.2 To create a new cryptographic key

> ⚠ 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.

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.*

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.

35.3 To delete a cryptographic key from the system

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.

After you have successfully revoked a cryptographic key, use the following instructions to delete the key from the system.

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.

> ℹ Note
>
> Once a cryptographic key is deleted from the system, it cannot be restored.

Related Information

To revoke a cryptographic key [page 505]
Cryptographic key status [page 502]

35.4 To revoke a cryptographic key

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.

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.

Once a cryptographic key is revoked, it can be safely removed from the system since no sensitive data objects require the key for decryption.

35.5 To mark cryptographic keys as compromised

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.

> **i Note**
>
> You can also mark a key as compromised after it has been revoked.

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.

     > **i 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

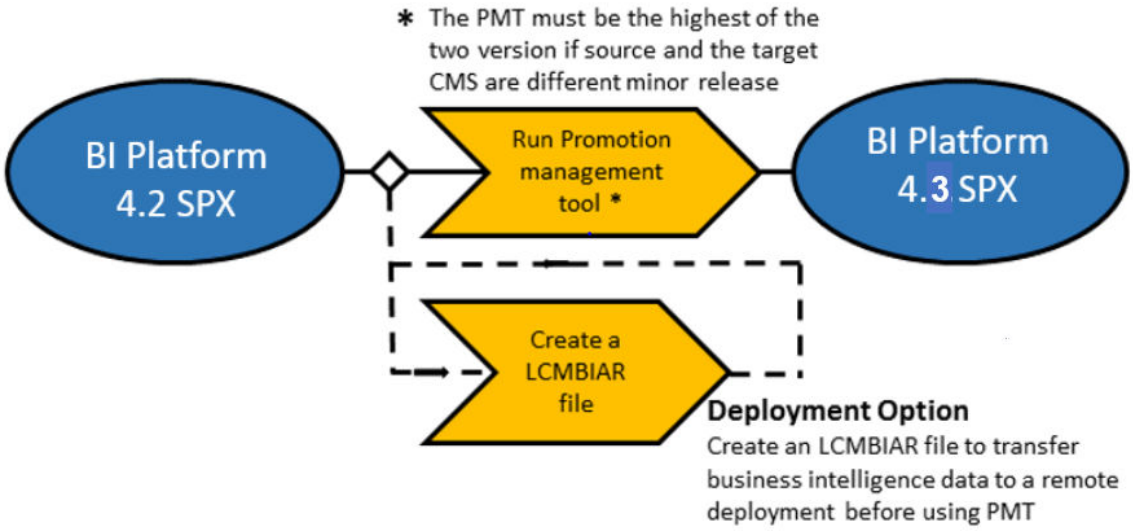
To revoke a cryptographic key [page 505]
Cryptographic key status [page 502]
To view objects associated with a cryptographic key [page 503]

36 Promotion Management

36.1 Promotion Management

36.1.1 Welcome to promotion management

36.1.1.1 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.

36.1.1.2 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.

36.1.1.3 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.

36.1.1.4 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.

36.1.2 Getting started with the promotion management tool

36.1.2.1 Accessing the promotion management tool

To access the promotion management tool, select *Promotion Management* from the CMC home page.

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.

36.1.2.2 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.
Rollback	Allows you to undo the promoted job on the destination system. **i 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.

Option	Description
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.

36.1.2.3 Using the Settings option

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.

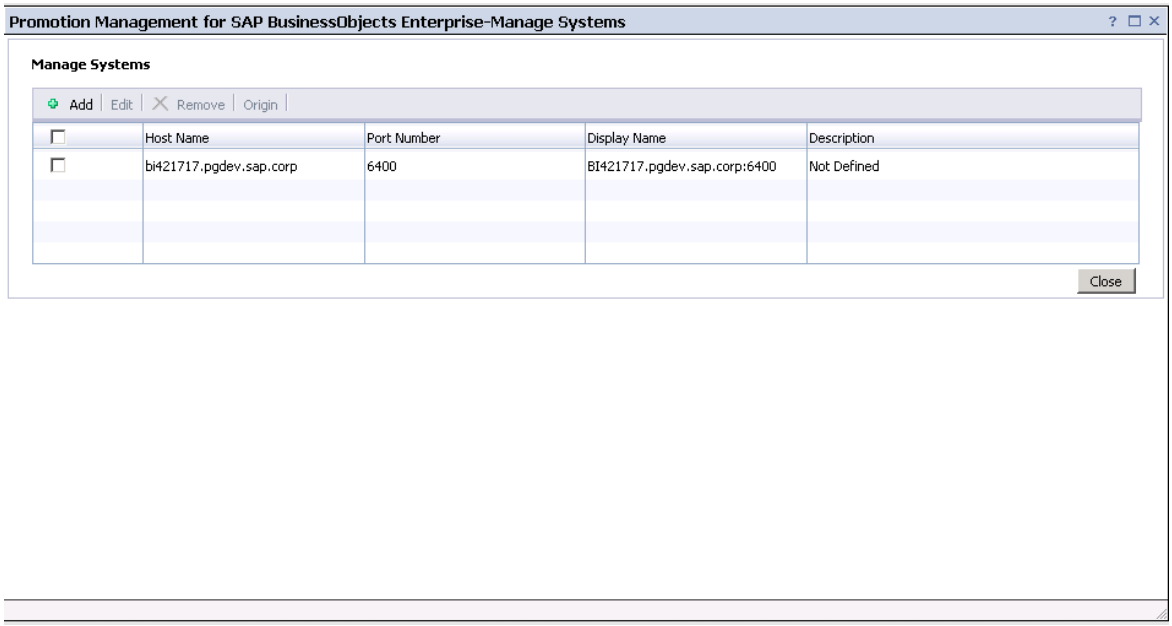
- *CTS settings* This option allows you to add the web service and SAP BW system information for the Enhanced Change and Transport System integration.

36.1.2.3.1 To use the Manage Systems option

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.

> **i 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.

> **i 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 513]
To use the Job Settings option [page 513]

36.1.2.3.2 To use the Rollback Settings option

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 513]

36.1.2.3.3 To use the Job Settings option

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.

> **i Note**
>
> The old job instances are deleted only when the job is executed the next time.

Related Information

To use Apache Subversion as the Version Management System [page 592]

36.1.2.3.4 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.

> **i 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.

36.1.2.3.4.1 To promote overrides

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 512].

To promote the overrides, complete the following steps:

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.

   > **i 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.

   > **i 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.

   > **i 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.

   > **i 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.

   > **i 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*.

36.1.2.3.4.2 To promote overrides using BIAR Files

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 512].

To promote the overrides through BIAR files, complete the following steps:

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*.

36.1.2.3.4.3 To promote overrides using CTS+

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 512].

To promote the overrides through CTS+, complete the following steps:

> **Note**
>
> Launch the promotion management tool using SAP authentication for this option to be available.

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. 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 to Active for the objects you want to promote, and click *Save*.
7. Click *Promote Overrides*.
   The *Promote Overrides* screen is displayed where the list of destination systems is displayed.
8. From the *Promotion Options* drop-down list, select *Promote with CTS+*.
9. Click *Promote*.
10. Release the overrides to the destination system by completing the following steps:
    a. Login to the domain controller of CTS+ and open the *Transport Organizer* Web UI. For more information on using the Transport Organizer Web UI, see Transport Organizer Web UI.

b. If the status of the request is *Modifiable*, click *Release* to release the transport request of the overrides. For more information on Releasing Transport Requests with Non-ABAP Objects, see Releasing Transport Requests with Non-ABAP Objects.
c. Close the *Transport Organizer* Web UI.

11. Import the overrides to the destination system by completing the following steps:
    a. Login to the Domain Controller of CTS+.
    b. Call the STMS transaction to enter the transport management system.
    c. Click on the *Import Overview* icon.

       The *Import Overview* screen is displayed and you can view the import queue items from all the systems.
    d. Click the System ID of the destination Promotion Management system.
       You can see the list of transport requests that can be imported to the system.
    e. Click *Refresh*.
    f. Import the relevant transport requests. For more information, see the Importing Requests documentation.
12. The promotion of overrides is complete.
13. Login to one of the destination systems using valid credentials.
    A list of all the promoted objects is displayed in "list of overrides". The status of these objects is Inactive.
14. Click the *Select* check box for the objects you want to edit, and click *Edit*.
15. Update the required values, and click *Done* .
    The state of the edited objects becomes Active.
16. Click *Save*.

36.1.2.3.5 Using the CTS Settings option

You can use this option to add web services and manage BW systems in your landscape. Refer to the To configure CTS+ settings in the promotion management tool [page 570] section for more information on using the CTS Settings Option and setting up CTS for usage with the promotion management tool.

36.1.3 Using the promotion management tool

When you launch the promotion management tool, by default, you are taken to the *Promotion Jobs* page.

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.

36.1.3.1 Creating and deleting folders

This section describes how to create and delete a folder in the promotion jobs home page.

36.1.3.1.1 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 520]
To delete a folder [page 520]

36.1.3.1.2 To delete a folder

This section describes how to delete a folder.

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 520]

36.1.3.2 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:

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 te 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 514]

36.1.3.2.1 To log onto a new CMS

This section describes how to log into a new CMS.

To log into a new CMS, complete the following steps:

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 520].
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 523]
To add an infoobject to a job [page 524]
To promote a job when repositories are connected [page 526]
To schedule a job promotion [page 532]

36.1.3.3 To create a new job by copying an existing job

This section describes how to create a new job by copying an existing job.

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 524]
To edit a job [page 523]
To promote a job when repositories are connected [page 526]

36.1.3.4 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.

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 524]
To edit a job [page 523]

36.1.3.5 To edit a job

This section describes how to edit a job.

> **i** Note
>
> 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.

While editing a job, you cannot change the name of the source system.

Related Information

To add an infoobject to a job [page 524]
To promote a job when repositories are connected [page 526]
To schedule a job promotion [page 532]

36.1.3.6 To add an infoobject to a job

Each job must include a set of infoobjects. Hence, you must add infoobjects to a job before you promote it to the destination system.

> **i 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.

To add an infoobject to a job, complete the following steps:

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 520] and To edit a job [page 523].
3. Click *Add Objects* if editing a job.

   > **i 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.

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 525]
To promote a job when repositories are connected [page 526]
To schedule a job promotion [page 532]

36.1.3.7 To manage the dependencies of a job

This section describes how to manage the dependents of an infoobject.

To manage the dependents of an infoobject, complete the following steps:

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 520] and To edit a job [page 523].
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 526]

6. Click *Apply Changes* to update the list of dependents and click *Apply Changes and Close* to save the changes.

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.

> **i** 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 526]

36.1.3.8 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.

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 525]

36.1.3.9 To promote a job when repositories are connected

This section describes how to promote a job from the source system to the destination system if both systems are live.

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, Workspace, Sets	Universes UNV, Connections, Sets
EPM Dashboard	Universes, Connections, Reports, and Analytics
BusinessView	DataFoundation
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 Fooundation (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 .

> **i 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.

> **i Note**
>
> By default, the *Include Federation Jobs Relationship* checkbox is selected.

To promote a job, complete the following steps:

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.

   > **i 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*.

   > **i 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.

   > **i 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.

   > **i 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.

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.

36.1.3.10 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.

> **i** Note
>
> You cannot use an LCMBIAR file that was created using the Import Wizard.

Related Information

Exporting a job to an LCMBIAR File [page 529]
Importing a job from an LCMBIAR File [page 530]

36.1.3.10.1 Exporting a job to an LCMBIAR File

This section describes how to export a job to an LCMBIAR file.

To export a job to an LCMBIAR file, complete the following steps:

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 520]
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*.

   > **i 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*.

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 532] section.

Related Information

To add an infoobject to a job [page 524]
To manage the dependencies of a job [page 525]

36.1.3.10.2 Importing a job from an LCMBIAR File

You can import a job from an LCMBIAR file. The LCMBIAR file is copied from the storage device to the destination system.

To import an LCMBIAR file, complete the following steps:

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.

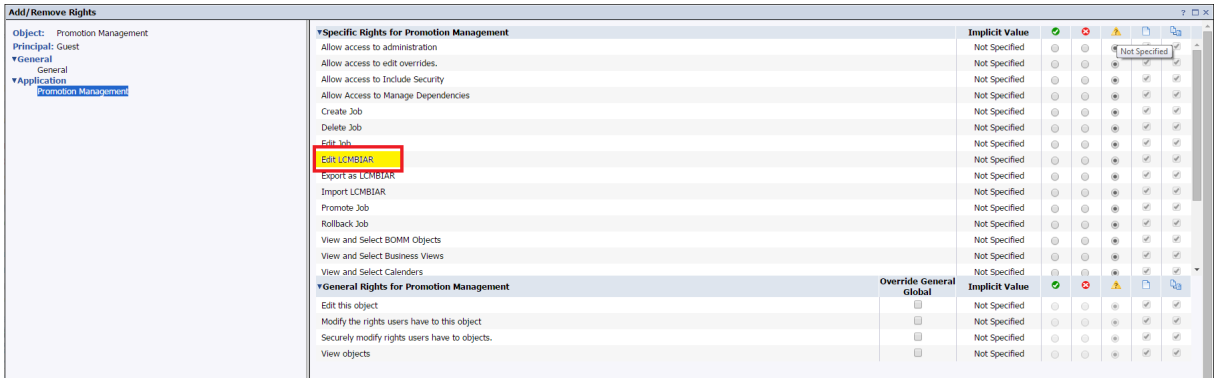
   You can also click the *Test Promote* option to view the objects to be promoted and the promotion status.

Related Information

To manage the dependencies of a job [page 525]

36.1.3.10.2.1 Selective retrieval of objects from an LCMBIAR file

To selectively retrieve objects from an LCMBIAR file, it is required that the user have *Edit LCMBIAR* right.



To selectively retrieve objects from an LCMBIAR file, perform the following:

1. Select the objects to be promoted.
2. Click *Promote*.

> **i** 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 544]
> - Selective promotion is not supported for live to live scenario.

36.1.3.11 To schedule a job promotion

This section describes how to schedule the promotion of a job. It also describes how to specify the recurrence options and parameters.

To schedule the promotion of a job instance, complete the following steps:

1. In the *Promote* dialog box, click the *Schedule* option.
2. Set the required schedule option and click *Schedule*.

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 529]

36.1.3.11.1 To update the recurring and pending job promotion instances

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:

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.

> **i 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 534]

36.1.3.12 To view the history of a job

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

To view the history of a job, complete the following steps:

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.

36.1.3.13 To roll back a job

The Rollback option allows you to restore the destination system to its previous state, after a job is promoted.

To roll back a job, complete the following steps:

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.

You can roll back only the most recent instance of a promotion job. You cannot roll back multiple job instances simultaneously.

36.1.3.13.1 To use the Partial Rollback option

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:

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*.

> **i** 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 591]

36.1.3.13.2 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.

> **i** 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 536]
To use the Partial Rollback option [page 534]

36.1.3.13.2.1 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*.

> **i** Note
>
> The jobs that were promoted using the source or destination system credentials are updated automatically.

Related Information

To roll back a job [page 534]
To use the Partial Rollback option [page 534]
To roll back a job after the password expires [page 535]

36.1.4 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.

36.1.4.1 To prepare the source and target systems

You must ensure that the source and target systems are configured optimally before promoting content.

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.

      > **i 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.

      > **i 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.

      > **i 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.

      > **i 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)

> **i Note**
>
> These sizing guidelines apply to most environments. However, the size of documents may affect resource requirements.

36.1.4.2 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.

    > **i 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).

    > **i 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.

    > **i** 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.

    > **i** Note
    >
    > Object security is preserved because it is inherited from folder security.

36.1.5 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 543] 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
```

36.1.5.1 To promote users and user groups (Job 1)

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.

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
   ```

36.1.5.2 To promote dependent objects (Job 2)

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

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
```

36.1.5.3 To promote primary objects (Job 3)

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.

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
```

> **i 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.

> **i 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.

36.1.5.4 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.

36.1.6 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

36.1.6.1 To run the command-line tool on Windows

To run the command line tool, complete the following steps:

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>`

     > i Note
     >
     > Enter the valid passwords when prompted.

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>`

36.1.6.2 To run the command-line tool on Unix

To run the command line tool, complete the following steps:

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>`

> **i** Note
>
> Enter the valid passwords when prompted.

36.1.6.3 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 548]
Source live CMS to a target live CMS [page 554]
Live CMS to a LCMBIAR file [page 551]
List of all the command line parameters [page 558]

36.1.6.3.1 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			

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
	`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
	`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

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
	`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
	`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

Parameter group	Parameter	LCMBIAR to Live	Live to LCMBIAR	Live to Live	Rollback
	`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
	`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 548]
Live CMS to a LCMBIAR file [page 551]
Source live CMS to a target live CMS [page 554]
List of all the command line parameters [page 558]

36.1.6.3.2 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 558].

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`

Parameter group	Parameter	Description
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: 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`

Parameter group	Parameter	Description
	`Destination_username`	User account that the tool must use to connect to the BI Platform CMS. Value: Valid user name Example: `Destination_username=admin LCM`
	`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 551]
Source live CMS to a target live CMS [page 554]
List of all the command line parameters [page 558]

36.1.6.3.3 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 558].

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`

Parameter group	Parameter	Description
	`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: 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 548]
Source live CMS to a target live CMS [page 554]
List of all the command line parameters [page 558]

36.1.6.3.4 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 558].

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 548]
Live CMS to a LCMBIAR file [page 551]
List of all the command line parameters [page 558]

36.1.6.3.5 List of all the command line parameters

The following table describes all the command line parameters.

> **i** 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` **Note** Mandatory for SAP authentication.	Required for SAP authentication only. Value: System ID Example: `LCM_systemID=systemID`
	`LCM_clientID` **Note** Mandatory for SAP authentication.	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`

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`

36.1.6.3.6 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 545] 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 558].

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`

36.1.6.4 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.

36.1.7 Using the Enhanced Change and Transport System

The Change and Transport System (CTS) organizes and customizes development projects in the ABAP Workbench, and then transports these changes between SAP Systems in your system landscape. The Enhanced Change and Transport System (CTS+) is an add-on to the CTS that promotes non ABAP content across CTS+ enabled non-ABAP repositories.

BI platform infoobjects can use SAP Business Warehouse content as a data source. The integration of CTS+ with the promotion management tool enables the handling of the BI platform repository, in a similar way to the SAP Business Warehouse (BW) repository, by using CTS transport requests to promote jobs. CTS+ provides an option to transport non-SAP objects within a system landscape. For example, objects created in the development system can be attached to a transport request and forwarded to other systems within the landscape.

For more information about the Change and Transport System, see Change and Transport System - Overview (BC-CTS)

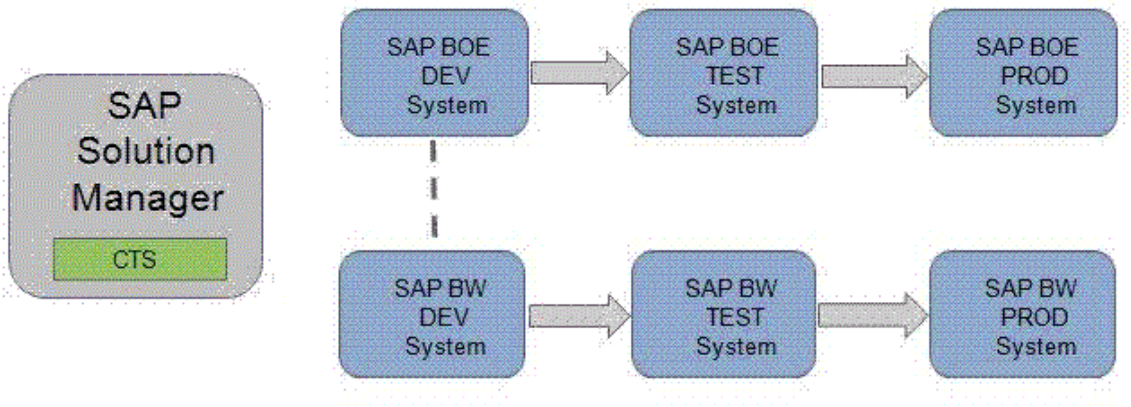
For more information about CTS+ and non ABAP transports, see Transporting Non-ABAP Objects in Change and Transport System

36.1.7.1 Prerequisites

The following are the prerequisites for transporting business intelligence content from system to another through CTS+:

1. BI platform 4.0 (or newer) is installed.
2. SAP Solution Manager 7.1 or SAP Solution Manager 7.0 EHP1 (minimum SP25) is installed and is used as the domain controller for CTS+, at least for the configuration of SAP BusinessObjects systems.
   For more information about configuring the transport domain, see Configuring the Transport Domain.
3. The CTS plug-in is installed on the SAP Solution Manager (CTS plug-in is taken from SL Toolset 1.0 SP02. We recommend that you use the latest available CTS plug-in).
   For more information on installing the required CTS plug-in, see the SAP Note: SAP Note 1533059.
4. *SAP Business Warehouse 7.0* (SPS 24 or higher) systems are installed. For more information, see SAP note SAP Note 1369301.
5. SAP Business Warehouse (SAP BW) transport landscape is configured in the Change and Transport System (CTS).
6. SAP Note 1692417 and SAP Note 1860594 have been implemented on the machine that hosts the CTS Deploy Web Service.

36.1.7.2 To configure the BI platform and CTS+ Integration



The Transport Management System (TMS) which is part of the Change and Transport System is used to transport changes between the SAP systems within a landscape. It manages the connected systems, their routes, and the imports into its systems. For more information about the Transport Management System, see Transport Management System (BC-CTS-TMS)

CTS+ enables collection of files from outside and their distribution within a transport landscape. The Transport Organizer Web UI, which is part of CTS+, manages the transport requests and the objects contained by it. For more information, see Transport Management System (BC-CTS-TMS)

You can integrate BI platform promotion management with CTS+ and SAP BW using CTS transport requests.

> **i** Note
>
> To enable the integration of the BI platform with SAP Solution Manager, you need to define "BOLM" application type in the SAP Solution Manager landscape.

Perform the following steps to integrate the BI platform and CTS+:

1. Activate the CTS export web service.
2. Configure CTS settings in the promotion management tool.
3. Configure the BI platform import system in SAP Solution Manager.

Related Information

To activate the CTS Export web service [page 570]
To configure CTS+ settings in the promotion management tool [page 570]
To configure the BI platform and CTS+ Integration [page 569]

36.1.7.2.1 To activate the CTS Export web service

To configure BI platform, you need activate CTS export web service in the SOA Management web tool.

1. To start the application, enter the transaction code SOAMANAGER in your SAP Solution Manager. After the required authentication is done, the SOA Management Console opens in a Web browser.

   For more information on SOA Management and the configuration of a service endpoint using SAP Solution Manager 7.0, see Configuring a Service Provider. For SAP Solution Manager 7.1, see Configuring a Service Provider.
2. On the *Application and Scenario Communication* tab, click *Single Service Configuration*.

   The CTS Export Web Service is named `EXPORT_CTS_WS`
3. In the *Configuration* tab, create or edit the service endpoint.
4. In the *Security* tab, configure the transport protocol and authentication method.
5. In the *Transport Settings* tab, define alternative access URL for the convenient access of the service endpoint.

36.1.7.2.2 To configure CTS+ settings in the promotion management tool

The following section describes the configuration steps to be performed in the CMC application to set up CTS+ for usage with the promotion management tool.

1. In the *Promotion Jobs* page, click *CTS Settings* and then click *BW Systems*.
2. In the *BW Systems* page, click *Add* to add a BW system to the landscape.
3. In the *Add System* page, enter the following details:
   - *Host BW SID*: specify the system ID (SID) of the host SAP BW/ABAP machine.
   - *Host Name*: specify the IP address of the host machine.
   - *System number*: enter the system number of the host system.
   - *Client*: refers to the system details of the client machine.
   - *User* and *Password*: specify the user name and password on the client machine in these fields.
   - *Language*: specify your choice of language in this field.
4. Click *OK* to add the system to your landscape.

   > **i Note**
   >
   > Once you've added a BW system to your landscape, you can use the *Edit* or *Delete* in the *BW Systems* page to modify the systems in your landscape.
5. In the *Promotion Jobs* page, click *CTS Settings* and then click *Web Service Settings*.
6. In the *Web Service Settings* page, enter the Web Service URL and user details.

   > **i Note**
   >
   > If you're not familiar with these details, obtain the same from the Solution Manager administrator.

7. Click *Save* and *Close* to complete adding the web service settings.
8. Create a mapping file for the BI platform promotion management CMS system.

   Complete the following steps in the BI platform development system to create a text file with connectivity details to enable the mapping:

   a. In the BI platform promotion management CMS, go to the root directory and create a folder with name **`LCM`** in the path `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/`
   b. Create a text file with name `LCM_SOURCE_CMS_SID_MAPPING.properties`, and enter either one of the following in the file:
      - `<Complete name of the SAP BI platform source system with domain>@<CMS port number> = <logical name for source system as used in CTS configuration >`
      - `<IP number of the SAP BI platform source system>@<CMS port number> = <logical name for source system as used in CTS configuration >`

   For example:

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> **i Note**
>
> In case of clustered environment, copy the `LCM_SOURCE_CMS_SID_MAPPING.properties` file to the system where Adaptive Processing Server is running.

For more information about performing configuration steps for non-ABAP systems, see Making Transport Settings in the Application.

36.1.7.2.3 To configure the BI platform import system in the SAP Solution Manager

1. Log on to the SAP Solution Manager system.
2. Enter transaction `stms` and press `Enter`.
3. Configure BOLM as the application type.
   a. Go to *Overview* > *Systems*.
   b. Go to *Extras* > *Application Type* > *Configure*.
   c. Choose *New Entries*.
   d. In the *Application Type* field, enter **`BOLM`**.
   e. Enter description.
   f. In the *Support Details* field, enter **`http://service.sap.com (ACH: BOJ-BIP-DEP)`**
   g. Choose *Table View* > *Save*.
   h. Confirm the prompt by choosing *Yes*.
4. To work with different languages, you can maintain translated text as follows:
   a. Choose *Goto* > *Translation*.
   b. Select the languages into which you want to translate the text.

c. Enter the translated values in the *Description* and *Support Details* fields.
d. Confirm the dialog box.
e. Choose *Continue*.
f. Choose *Table View* > *Save*.
g. Confirm the prompt.

The TMS domain is now ready to support usage of business intelligence content in CTS.

5. In CTS+, define the BI platform source system as an export system.

> **i Note**
>
> For more information on creating a non-ABAP system as a source system, see Defining and Configuring Non-ABAP Systems

6. In CTS+, configure the BI platform import system by completing the following steps:

> **i Note**
>
> You can define a SID as a reference to the BI platform import system.

a. Create a non-ABAP system as an import system.
   For more information, see Defining and Configuring Non-ABAP Systems.
b. Specify the deployment method as *Other* and deselect all other options.
c. Choose *Save*.
d. Confirm the distribution dialog box.
   The table view to configure the import system settings appears.
e. Choose *Edit* > *New Entries*.
f. In the "Change View CTS: System details for handling of application types" screen, perform the following steps:
   1. In the *Deploy Method* field, select *application specific Deployer (EJB)*.
   2. In the *Deploy URI* field, enter the following URI: **`http://<BOE web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`**
      where
      - "BOE web server name" is the name or IP address of the machine where the BI platform web server is running.
      - "Web server port" is the port number of the BI platform web server.
      - "BOE destination name" is the name of the machine on which the target BI platform Central Management Server (CMS) is running.
      - "CMS port" is the port number of the target CMS.
      - "BOE authentication type" is the type of user authentication for importing business intelligence content. The supported authentication types are secEnterprise, secLDAP, secWinAD, and secSAPR3.
   3. In the *User* field, enter the BI platform user name.
   4. In the *Password* field, enter the BI platform password.
   5. Choose *Save* to save the settings.

If you require more than one import system, repeat the steps above to create all destination systems required. To configure transport routes between the source and target system after the creation of the destination systems, see Configuring Transport Routes

36.1.7.2.4 To export from BI platform to CTS+ with SSL

36.1.7.2.4.1 To configure SSL for CTS+

To configure SSL for CTS+, you must configure SSL on Application Server ABAP. For more information, see Configuring the SAP Web AS for Supporting SSL.

36.1.7.2.4.2 To configure the client-side SSL certificate

To configure the client-side SSL certificate, you must either import the server certificate or the trusted CA certificate into the JVM keystore.

1. Back up the `cacerts` files from the `<INSTALLDIR>\win64_x64\sapjvm\jre\lib\security` directory.
2. Import the certificate into the Tomcat JVM that hosts the `BOE.war` file using the following parameters:

```
<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer
-keystore cacerts
```

3. Restart Tomcat.

36.1.7.2.4.3 To configure the CTS+ Export Web Service

To configure the HTTPS-enable CTS+ Export Web Service (`EXPORT_CTS_WS`) you can create a new HTTPS endpoint.

> **i** Note
>
> Alternatively, you can switch your existing HTTP endpoint to use HTTPS.

1. Use transaction code **`soamanager`**, and on the *Provider Security* tab, under *Communication Security*, select *SSL over HTTP (Transport Channel Security)* and Under *Transport Channel Authentication*, select *User ID/Password*.
2. On the *Transport settings* tab, under *Transport Binding*, select *HTTPS* for *Calculated Protocol*.

36.1.7.2.4.4 To configure promotion management for SSL

> **→** Remember
>
> Import the server certificate or the trusted CA certification into the JVM keystore.

1. In the CMC, on the *Promotion Management* tab, click *Settings* > *CTS Settings* > *Web Service Settings*.
2. Ensure that the *Web Service URL* parameter includes `https://` and the port number configured above.

> **Note**
>
> *Promote via CTS* will not be displayed in the *Job destination* list or in the *Overrides* dialog box if the specified URL cannot be reached. If the SSL handshake between promotion management and CTS+ fails, an error will be recorded in the CMC log file.

36.1.7.2.5 To import from CTS+ to BI platform with SSL

36.1.7.2.5.1 To configure BI platform Tomcat to use HTTPS

To configure BI platform Tomcat to use HTTPS, you must perform the following steps on the machine where BI platform is installed.

1. Create a server key pair, a certificate, and a keystore.
   a. Run `<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe` with the following parameters:

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   serverkeystore.jks -storetype JKS
   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b. When prompted, enter the following information:
      - Your first and last names
      - The name of your organizational unit
      - The name of your organization
      - The name of your city or locality
      - The name of your state or province
      - The two-letter country code for this unit

      A formatted string will be displayed (for example, `CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA`). Type **yes** and press `Enter` to confirm.
2. Send the server certificate request to a Certification Authority (CA).
3. Import the signed server certificate into the server keystore using the following parameters:

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts
   -file server.crt
   ```

4. Configure the Tomcat configuration file `server.xml` to enable HTTPS and to use the server keystore that you have created.
5. Restart Tomcat and test the connection by accessing the following URL in a browser: `https://<SERVERNAME>:<SSLPORTNUMBER>`

Related Information

To configure SSL for CTS+ [page 573]

36.1.7.2.5.2 To configure CTS+ for SSL

To configure CTS+ for SSL, you must create an SSL client PSE and import a certificate into it.

Related Information

To configure SSL for CTS+ [page 573]

36.1.7.2.5.3 To update the test and production systems in CTS+ to use HTTPS

To enable HTTPS on the test and production systems, perform the following steps:

1. Use the STMS transaction code.
2. Click *System Overview*.
3. Select your test or profuction system and click *Goto* > *Application Types* > *Deployment Method*.
4. Ensure that the *Deploy URI* parameter includes `https://` and a configured HTTPS port number.

36.1.7.3 To promote a job using CTS

This section describes the workflow that the promotion management tool supports for promoting BI platform Central Management Server (CMS) objects from the source system to a destination system using the Change Transport System. To use CTS to promote a job, complete the following steps:

1. Launch the promotion management tool using SAP authentication, and create a job.

   For more information on creating a new job, see the "Creating a Job" section in the related links below .

   > **Note**
   >
   > Ensure that you select "SAP" as the authentication type in the source system login screen.

2. From the *Destination* drop-down list, select the *promote via CTS* option.

3. Click *Create*.
   The *Add Objects from the System* screen appears. Here the folders and subfolders are displayed in a tree structure.
4. Navigate to the folder from which you want to select the infoobject.
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* screen, click *Add and Close*.
   The infoobject is appended to the job and the *Promotion Jobs* screen appears.

   > **i Note**
   >
   > On the Promotion Jobs screen you can do the following:
   > - Use the *Add Objects* option to add more info objects to the job. For more information, see Adding an Infoobject to a job.
   > - Use the *Manage Dependencies* option to manage the dependencies of the info object you have selected. The SAP BW dependencies of the object are displayed on the UI and available for the user to select.
   >   For more information, see Managing Job Dependencies.

6. Click *Promote*.
   The *Promote* screen appears which displays the ID, owner and a short description of the currently set default transport request.
7. You can use the *Transport Requests* hyperlink to do the following:
   - View details of the transport request.
   - Change settings of the default transport request.
   - Choose a different transport request.
   - Create a transport request.

   1. Click the *Transport Requests* hyperlink to open the *Transport Organizer* Web User Interface.
   2. If prompted for logon credentials, log on using valid user credentials for the CTS domain controller system.
   3. Refresh the *Promote* Screen to view your updates.

   For more information about using the *Transport Organizer* Web UI, see Transport Organizer Web UI
8. To view the details of the dependencies of the SAP BW objects, click the *Second level dependencies* hyperlink.

   > **i Note**
   >
   > Only the objects that are locked in a request are displayed when you click the *Second level dependencies* hyperlink. If the request has been released you can not view any dependencies. In addition, this hyperlink is grayed out if there are no active second level dependencies.

9. Click *Promote*.
10. Close the job.
    The promotion management main screen is displayed. The status of the job that you created is now *Exported to CTS*.
11. Release the BI platform object to the destination system by completing the following steps:
    a. Click the link displayed in the status column of the job that you want to promote.
       The *Promotion Status* window appears.

b. Click *State of Request*.
The *Transport Organizer* Web UI appears.
c. If the status of the request is *Modifiable*, click *Release* to release the transport request of the BI platform object . For more information about releasing transport requests containing non-ABAP objects, see Releasing Transport Requests with Non-ABAP Objects
d. Close the *Transport Organizer* Web UI.

12. To view the dependencies for the SAP BW objects, click *List of BW dependencies* hyperlink.

> **i Note**
>
> We recommend talking to the SAP BW team to get updates on the SAP BW dependencies and their release as these objects are worked on by the team.

13. Close the *Promotion Status* window.
14. Import the BI platform object to the destination system by completing the following steps:
    a. Log on to the CTS+ domain controller.
    b. Call the **STMS** transaction to enter the transport management system.
    c. Click on the *Import Overview* icon.
    The *Import Overview* screen appears and you can view the import queue items from all the systems.
    d. Choose the system ID of the destination Promotion Management system.
    You can see the list of transport requests that can be imported to the system.
    e. Click *Refresh*.
    f. Import the relevant transport requests. For more information, see Importing Requests

    For general information about importing transport requests with BOLM content, see Importing Transport Requests with Non-ABAP Objects
15. If the object that you selected has SAP BW dependencies, perform the following steps:
    a. Release the SAP BW dependencies to the destination system by completing the following steps:
        1. Log on to the SAP BW source system.
        2. Call SE09 transaction. The *Transport Organizer* screen appears.
        3. Click *Display* .The SAP BW request is displayed.
        4. Click the SAP BW request and expand it to view the tasks created for the dependencies.
        5. Right click the request associated with the primary SAP BW object and select *Release Directly*. Repeat this step to release all the tasks associated to each dependent separately.
        6. Right click on the request associated to the primary BW object and select *Release Directly*.
        7. Refresh the screen until all the requests are released.

        > **i Note**
        >
        > You can view the logs for a request by double clicking it.

    b. Import the SAP BW dependencies to the destination system by completing the following steps:
        1. Log on to the SAP BW destination system.
        2. Call the STMS transaction to enter the transport management system.
        3. Click the *Import Overview* icon. The *Import Overview* screen appears.
        4. Double-click the system ID for the SAP BW destination. You can see the list of transport requests that can be imported to the system.
        5. Import the relevant transport requests. For more information, see Importing Requests
        For more information about Transports with Import Queues, see Transports with Import Queues

16. Log on to the destination system to view the status of the job you promoted.

For information on generic CTS, see Configuring Target Systems for Further Applications

Related Information

To create a job [page 520]
To manage the dependencies of a job [page 525]

36.1.8 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.

> i 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.

> i 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.

36.1.8.1 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.

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.

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.

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

36.1.8.2 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 Management Wizard	Promotion Management using the Command Line option	Promotion Management within the Central Management Console
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

> **i Note**
>
> LCMBIAR files are compatible with each promotion management option, regardless of the promotion management option you select.

36.1.8.2.1 Defining the promotion management settings

1. Specify the promotion management settings you require. Information to help you is provided here:

Setting	Description
Temporary Folder	**i 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 • 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*

36.1.8.3 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.

36.1.8.3.1 Promoting objects from a live CMS source system to an LCMBIAR file

To promote objects from a live CMS to an LCMBIAR file:

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.

   > **i Note**
   >
   > If you encrypt the LCMBIAR file, the promotion process takes more time.

5. Click *Next* to select the objects you want to export.

36.1.8.3.2 Promoting objects from a live CMS source system to a live CMS destination system

To promote objects from a live CMS source system to a live CMS destination system:

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.

36.1.8.3.3 Promoting objects from an LCMBIAR file to a live CMS destination system

To promote objects from an LCMBIAR file to a live CMS:

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.

   > **i** Note
   >
   > If you encrypt the LCMBIAR file, the promotion process takes more time.

5. Click *Next* to select the objects you want to import.

36.1.8.4 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.

36.1.8.4.1 Promoting the full content

To promote the full content from the source system to the destination system:

1. Select *Full content promotion*.

   All the objects are selected for the promotion.
2. Click *Next* to review the content you have selected.

36.1.8.4.2 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.

36.1.8.4.2.1 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. **i Note** The option is checked by default.
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.

Security	Description
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 group 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.

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.

36.1.8.4.2.2 Promoting selective content

To promote the selective content from the source system to the destination system:

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

   > **i** 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.

36.1.8.5 Dependencies

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:

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.

36.1.8.6 Summary

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:

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.

36.1.8.7 (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`

36.1.8.7.1 Configuring SSL settings

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`

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 **i Note** Entering this value enables SSL communication.
`-DcertDir`	The location of keys and certificates
`-DtrustedCert`	The name of the trusted certificate file **i 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
```

36.1.8.7.2 Configuring parameters

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`

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.
`-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.

Parameter	Value
`-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
```

36.1.8.8 Promotion Management Wizard on Linux

You can run Promotion Management Wizard on Linux.

Before you start Promotion Management Wizard on Linux, ensure that the Java runtime is set in the system PATH variable.

To start Promotion Management Wizard on Linux, perform the following steps:

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.

36.2 Version Management

36.2.1 To manage different versions of BI resources

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:

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*.

   > **i** 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.

   > **i** 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.

    > **i** 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.

    > **i** 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.

36.2.2 To use Apache Subversion as the Version Management System

You can set Apache Subversion as yourVersion Management System and configure the settings from Central Management Console.

1. In the CMC, click *Applications*.
2. Double click *VMS*.
   The Version Management Settings screen is displayed.
3. Select *VMS Settings*.
4. From the *Version Management Systems* list, select *Subversion*.
   The server port number, password, repository name, server name, user name, the name of the workspace directory and the name of the installation path (that were provided during the promotion management tool installation process) are displayed in the appropriate fields.

5. Modify the fields as required.

   > **Note**
   >
   > Ensure that you enter the install path that contains the `.exe` file.

   On Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion`

   On Unix: `<INSTALLDIR>/sap_bobj/enterprise_40/subversion/bin`
6. Select *SVN*, *HTTP*, or *HTTPS*.

   > **Note**
   >
   > For more information on connecting to Subversion using HTTPS see the *Apache Subversion Documentation*.
7. (Optional) Click *Test VMS* to validate your VMS settings.
8. Click *Save*.

   > **Note**
   >
   > - If you want Subversion to be your default VMS, select *Use as Default VMS*.
   > - If you have modified the fields, restart the Adaptive Processing Server.

36.2.3 To compare different versions of the same job

You can view the differences between two versions of the same job by completing the following steps:

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.

36.2.4 To upgrade Subversion content

If you have old Subversion content that was created using a previous version of the BI platform, you can upgrade your content to the latest version by following these steps:

1. Log on to the VMS on the SAP BusinessObjects Enterprise 4.2 machine.
2. Check-in any object. For example, check in the administrator and guest objects twice.

3. In CMC, click *Users* and verify that `2` is displayed in the in VMS and CMS version number.
4. Log off from the VMS.
5. Go to the command prompt, navigate to `C:\Program Files\Subversion\bin`, and run the export command: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Copy the `dumrepo` file to the BI platform machine
7. Go to the command prompt on the BI platform machine, navigate to `C:\Program Files (x86)\SAP`, and execute the following commands:

   ```
   svnadmin.exe load "C:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
   ```
8. After the commands have been successfully executed, restart the SIA.
9. Login to the CMC and click *Version management*.
10. Click on *Users*, and verify that the VMS version is `2`.
11. Select the *Administrator* object, and then click *Get Latest Version*.
12. The version number on the VMS and CMS are now the same.

    For more information on Apache Subversion upgrade, please refer to Apache Subversion 1.10 Release Notes .

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

© 2023 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.

THE BEST RUN SAP