



SAP BusinessObjects Enterprise Administrator's Guide

Copyright

© 2013 SAP AG 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 AG. The information contained herein may be changed without prior notice. Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group 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 AG in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

2013-03-04



Contents

Chapter 1	Getting Started	25
	About this help.....	26
	Who should use this help?.....	26
	About BusinessObjects Enterprise.....	26
	What's new in BusinessObjects Enterprise XI 3.1?.....	27
	Where should I start?.....	29
	Planning or performing your first deployment.....	29
	Configuring your deployment.....	30
	Changing your deployment's architecture.....	30
	Improving your system's performance.....	31
	Working with objects in the CMC.....	31
	SAP BusinessObjects Enterprise guides.....	32
Chapter 2	Architecture	35
	Architecture overview.....	36
	Enterprise infrastructure.....	38
	BusinessObjects Enterprise web services.....	39
	BusinessObjects Enterprise management services.....	41
	BusinessObjects Enterprise storage services.....	42
	BusinessObjects Enterprise processing services.....	43
	Server Intelligence	46
	Life-Cycle Management (LCM).....	47
	Clients.....	48
	Browser-based web application clients.....	49
	Desktop client applications.....	53
	Services.....	60

Contents

Service Categories.....	61
Adaptive Job Server.....	73
Adaptive Processing Server.....	74
Central Management Server.....	74
Connection Server.....	76
Crystal Reports Cache Server.....	77
Dashboard Analytics Server.....	78
Dashboard Server.....	79
Desktop Intelligence Cache Server	79
Desktop Intelligence Job Server.....	80
Desktop Intelligence Processing Server	80
Event Server.....	81
File Repository Servers	81
Job Servers.....	83
List of Values Job Server.....	84
Multi-Dimensional Analysis Services (MDAS) Server	84
PM Metrics Server.....	85
PM Repository Server.....	85
PM Rules Server.....	86
Predictive Analysis Server	86
Process Analysis Server.....	87
Program Job Server.....	87
Publication Job Server.....	88
Report Application Server.....	88
Sets Profile Server	89
Sets Query Server	89
Web Intelligence Processing Server.....	90
Web Application Container Server (WACS).....	90
Xcelsius Cache Server.....	91
Web application servers.....	92
Java SDK.....	94

Contents

.NET SDK.....	97
Web Services	99
Web Application Container Service (WACS).....	101
Databases	102
System databases.....	102
Reporting databases.....	103
Auditing database.....	104
Authentication and single sign-on.....	105
Central Management Server (CMS) security.....	105
Security plug-ins.....	106
Authentication and authorization.....	107
Information Workflows	110
Authentication.....	110
Scheduling.....	111
Viewing.....	117
 Chapter 3 Security Concepts	 125
Security overview.....	126
Authentication and authorization.....	127
Primary authentication.....	128
Single sign-on support.....	130
Security plug-ins.....	134
Processing extensions.....	136
Active trust relationship.....	137
Logon tokens.....	137
Ticket mechanism for distributed security.....	138
Sessions and session tracking.....	139
CMS session tracking.....	140
Environment protection.....	140
Web browser to web server.....	140
Web server to BusinessObjects Enterprise.....	141

Contents

	Auditing web activity.....	141
	Protection against malicious logon attempts.....	141
	Password restrictions.....	142
	Logon restrictions.....	142
	User restrictions.....	143
	Guest account restrictions.....	143
Chapter 4	Managing Licenses	145
	Overview.....	146
	Managing license information.....	146
	To view license information.....	146
	Adding a license key.....	146
	To add a license key.....	146
	Viewing current account activity.....	147
	To view current account activity.....	147
Chapter 5	Managing and Configuring Servers	149
	Server management overview.....	150
	BusinessObjects Enterprise administrative tools.....	151
	Working with the Servers management area in the CMC.....	152
	About Web Application Container Servers.....	157
	About Server Intelligence.....	158
	Server management: what's new in this version of BusinessObjects Enterprise.....	159
	Working with nodes.....	162
	To add a node.....	163
	To remove servers from a new node.....	165
	Recreating a Server Intelligence Agent on a local machine.....	165
	Viewing and changing the status of servers.....	167
	To view a server's status.....	168

Contents

Starting, stopping, and restarting servers.....	168
Stopping a Central Management Server.....	171
Enabling and disabling servers.....	172
Adding, cloning, and deleting servers.....	173
Adding a server.....	174
Cloning servers.....	175
Deleting a server.....	177
Server groups.....	178
Creating a server group.....	178
Working with server subgroups.....	179
Modifying the group membership of a server.....	181
User access to servers and server groups.....	181
Configuring server settings.....	183
To change a server's properties.....	184
Working with configuration templates.....	184
Configuring server network settings.....	187
Changing the connect port used by Tomcat.....	197
Managing CMS system database connections.....	198
Copying data from one CMS system database to another.....	198
Preparing to copy a CMS system database.....	204
Deleting and recreating the CMS system database.....	206
Selecting a new or existing CMS database.....	209
Setting root directories and idle times of the File Repository Servers.....	211
Modifying performance settings.....	212
Configuring destinations for job servers.....	212
Configuring Windows processing servers for your data source.....	219
Configuring UNIX processing servers for your data source.....	220
Adding and removing Windows server dependencies.....	227
Changing the system user account.....	227
Configuring tracing for servers.....	228
To configure server tracing through the BO_trace.ini file.....	229

Contents

To configure server tracing through the command line.....	232
Configuring servers for SSL.....	235
Creating key and certificate files.....	236
Configuring the SSL protocol.....	239
Clustering Central Management Servers.....	241
Adding a CMS to a cluster.....	243
Adding a new node to a cluster.....	243
Adding clusters to the web.xml file.....	244
Changing the name of a CMS cluster.....	245
Backing up and restoring server configuration settings.....	247
To back up server configuration settings to a BIAR file.....	248
To restore server configuration settings.....	248
To import nodes from one cluster to another	260
 Chapter 6 Configuring Third-Party Authentication	 263
Using NT Authentication	264
Using NT user accounts and groups.....	264
Windows NT security plug-in.....	264
NT user account and group administration.....	265
Mapping NT user accounts and groups.....	266
Modifying the web.config file for NT single sign-on.....	274
Using LDAP authentication.....	275
Managing LDAP accounts.....	275
Using AD authentication.....	294
Windows AD security plug-in.....	296
Using AD users and groups.....	296
Configuring manual AD authentication.....	304
Configuring AD single sign on.....	330
Enabling Trusted Authentication.....	371
Configuring the server for Trusted Authentication.....	372
Configuring Trusted Authentication for the client.....	373

	Configuring Trusted Authentication for Business Process BI.....	380
Chapter 7	Working with Federation	381
	Federation.....	382
	Federation terms.....	384
	BI application	384
	Destination site	384
	Local.....	384
	Locally run completed instances	384
	Multiple Origin sites	385
	One-way replication	385
	Origin site	385
	Remote.....	385
	Remote Connection.....	385
	Remote Scheduling.....	385
	Replication.....	386
	Replication Job.....	386
	Replication List.....	386
	Replication Object.....	386
	Replication package.....	386
	Replication refresh.....	387
	Two-way replication.....	387
	Managing Replication Lists.....	387
	Creating Replication Lists.....	388
	Modifying Replication Lists.....	393
	Managing Remote Connections.....	394
	Creating Remote Connections.....	394
	Modifying Remote Connections.....	396
	Managing Replication Jobs.....	397
	Creating a Replication Job.....	398
	Scheduling a Replication Job.....	401

Contents

Modifying a Replication Job.....	401
Viewing a log after a Replication Job.....	402
Managing security rights.....	403
Rights required on the Origin site.....	404
Rights required on the Destination site.....	405
Federation specific objects.....	405
Replicating security on an object.....	406
Replicating security on an object using access levels.....	407
Replicating third-party users and groups.....	408
Replicating universes and universe connections.....	409
Managing Object Cleanup.....	410
How to use Object Cleanup.....	411
Object Cleanup limits.....	411
Object Cleanup frequency.....	412
Replication types and mode options.....	413
One-way replication	413
Two-way replication	414
Refresh from Origin or Refresh from Destination.....	414
Managing conflict detection and resolution.....	416
One-way replication conflict resolution.....	417
Two-way replication conflict resolution.....	419
Using Web Services in Federation.....	423
Session variable	423
File caching	423
Custom deployment	424
Remote scheduling and locally run instances.....	425
Remote scheduling.....	425
Locally run instances.....	427
Instance share.....	428
Importing and promoting replicated content.....	429
Importing replicated content.....	429

Contents

	Importing replicated content and continuing replication	430
	Promoting content from a test environment.....	431
	Re-pointing a destination site.....	431
	Best practices.....	432
	Current release limitations.....	436
	Troubleshooting error messages.....	437
Chapter 8	Working with Firewalls	443
	Understanding communication between BusinessObjects Enterprise components.....	444
	Overview of BusinessObjects Enterprise servers and communication ports.....	444
	Communication between BusinessObjects Enterprise components ..	447
	Configuring BusinessObjects Enterprise for firewalls.....	457
	To configure the system for firewalls.....	458
	Examples of typical firewall scenarios.....	461
	Example - Application tier deployed on a separate network.....	462
	Example - Rich client and database tier separated from BusinessObjects Enterprise servers by a firewall.....	465
Chapter 9	Working with Web Application Container Servers	469
	Web Application Container Server (WACS).....	470
	Do I need WACS?.....	471
	What are the advantages of using WACS?.....	472
	Common Tasks.....	473
	Adding or removing additional WACS to your deployment.....	476
	Installing WACS.....	477
	Adding a new Web Application Container Server.....	479
	Cloning a Web Application Container Server	480
	Deleting WACS servers from your deployment.....	481
	Adding or removing services to WACS.....	481

Contents

To add a CMC service to a WACS.....	481
To remove a CMC service from a WACS.....	482
Configuring HTTPS/SSL.....	483
To generate a PKCS12 certificate file store.....	484
To generate a Certificate Trust List.....	485
To configure HTTPS/SSL.....	486
Supported authentication methods.....	489
Configuring AD Kerberos for WACS	489
Enabling Kerberos authentication in the Windows AD plug-in for WACS.....	490
Creating configuration files.....	491
Configuring WACS for AD Kerberos.....	495
Troubleshooting Kerberos.....	495
WACS and your IT environment.....	497
Using WACS with other web servers.....	497
Using WACS with a load balancer.....	498
Using WACS with a reverse proxy.....	498
Using WACS with firewalls.....	500
Configuring WACS on a multihomed machine.....	500
Troubleshooting.....	501
To view server errors.....	501
To view system metrics.....	502
To view the state of a WACS.....	503
Resolving port conflicts.....	503
To change memory settings.....	506
To change the number of concurrent requests.....	507
To restore system defaults.....	507
To prevent users from connecting to WACS through HTTP.....	508
WACS properties.....	508

Chapter 10	Modifying Default Security Behavior	509
	BusinessObjects Enterprise and reverse proxy servers	510
	Introduction to reverse proxy servers.....	510
	Supported reverse proxy servers	511
	Understanding how BusinessObjects Enterprise web applications are deployed	511
	Configuring reverse proxy servers for BusinessObjects Enterprise web applications.....	512
	To configure the reverse proxy server	513
	Detailed instructions for configuring reverse proxy servers for BusinessObjects Enterprise.....	513
	To configure Apache 2.2 reverse proxy server for BusinessObjects Enterprise.....	515
	To configure WebSEAL 6.0 reverse proxy server for BusinessObjects Enterprise.....	516
	To configure Microsoft ISA 2006 for BusinessObjects Enterprise.....	517
	Special configuration for BusinessObjects Enterprise in reverse proxy deployments.....	521
	Enabling reverse proxy for Developer Suite Web Services.....	521
	Enabling the root path for session cookies for ISA 2006.....	524
	Enabling reverse proxy for BusinessObjects Live Office.....	528
	Enabling reverse proxy for Business Process BI Web Services.....	529
Chapter 11	Improving Performance	531
	Improving performance.....	532
	Assessing your system's performance.....	532
	Assessing user needs.....	533
	Analyzing server metrics.....	534
	Resolving performance issues.....	544
	Performance risks and solutions.....	546

Contents

Improving Publishing performance.....	560
General deployment recommendations.....	561
Configuring servers in the CMC to optimize Publishing performance.....	561
 Chapter 12 Managing Auditing	 567
How does auditing work?.....	568
Configuring auditing.....	574
Which events can I audit?.....	577
Enabling auditing of user and system events.....	593
To enable auditing events for client applications.....	596
Auditing Configuration Template.....	596
To set the Configuration template.....	597
Configuring the universe connection.....	598
Using sample auditing reports.....	599
Controlling synchronization of auditing actions.....	600
Optimizing system performance while auditing.....	601
 Chapter 13 Auditing Reports	 603
Using auditing reports.....	604
Why are reports important?.....	604
Auditing report names.....	607
Viewing sample auditing reports.....	619
Creating custom auditing reports.....	620
Auditing database schema reference.....	620
Audit_Event.....	620
Audit_Detail	621
Server_Process.....	622
Event_Type.....	623
Application_Type.....	624
Detail_Type tables.....	624

Event and Detail reference tables.....	625
Chapter 14 Server Command Lines	645
Command lines overview.....	646
Standard options for all servers.....	647
UNIX signal handling.....	650
Central Management Server.....	650
Central Configuration Manager (CCM).....	655
Crystal Reports Processing Server and Crystal Reports Cache Server...	656
Job servers.....	659
Report Application Server.....	662
Web Intelligence Processing Server.....	666
Input and Output File Repository Servers.....	668
Event Server.....	671
Chapter 15 UNIX Tools	673
Script utilities.....	674
ccm.sh.....	674
cmsdbsetup.sh.....	680
configpatch.sh.....	680
serverconfig.sh.....	680
uninstallBOBJE.sh.....	682
Script templates.....	682
startservers.....	682
stopservers.....	683
silentinstall.sh.....	683
Scripts used by BusinessObjects Enterprise.....	684
bobjerestart.sh.....	684
env.sh.....	684
env-locale.sh.....	684

Contents

	initlaunch.sh.....	685
	patchlevel.sh.....	685
	postinstall.sh.....	686
	setup.sh.....	686
	setupinit.sh.....	686
Chapter 16	BIAR Command Line Tool	687
	Biar Command Line Tool.....	688
	The Biar Engine Command Line Tool's Properties File	691
	To use the BIAR Command Line Tool.....	697
Chapter 17	Working with the Central Management Console	699
	Overview.....	700
	Using the CMC.....	700
	Logging on to the CMC.....	701
	Navigating within the CMC.....	702
	Setting CMC preferences.....	702
	Making initial security settings.....	705
	Setting the Administrator password.....	705
	Disabling a user account.....	706
Chapter 18	Setting Rights	707
	How rights work in BusinessObjects Enterprise.....	708
	Access levels.....	709
	Advanced rights settings.....	709
	Inheritance.....	710
	Type-specific rights.....	717
	Determining effective rights.....	719
	Managing security settings for objects in the CMC.....	720
	To view rights for a principal on an object.....	720

Contents

To assign principals to an access control list for an object.....	722
To modify security for a principal on an object.....	722
To set rights on a top-level folder in BusinessObjects Enterprise.....	723
Checking security settings for a principal.....	724
Working with access levels.....	728
Choosing between View and View On Demand access levels.....	731
To copy an existing access level.....	733
To create a new access level.....	733
To rename an access level.....	733
To delete an access level.....	734
To modify rights in an access level.....	734
Tracing the relationship between access levels and objects.....	736
Managing access levels across sites.....	736
Breaking inheritance.....	738
To disable inheritance.....	739
Using rights to delegate administration.....	740
Choosing between Modify the rights users have to objects options...	742
Owner rights.....	744
Summary of recommendations for rights administration.....	745

Chapter 19 **Managing Users and Groups** **747**

Account management overview.....	748
User management.....	748
Group management.....	749
Available authentication types	751
Managing Enterprise and general accounts.....	753
To add subgroups.....	758
Adding users to groups.....	760
Changing password settings.....	761
Enabling Trusted Authentication.....	763
Granting access to users and groups.....	765

Controlling access to user inboxes.....	765
Configuring the InfoView logon screen.....	765
Managing aliases.....	767
Chapter 20 Managing Applications	773
Overview.....	774
Setting user rights on applications.....	774
Managing Discussions settings.....	775
To manage Discussions settings in the CMC	775
To search for a discussion thread.....	775
To sort your discussion thread search results.....	777
To delete a discussion thread.....	778
Setting user rights.....	779
Managing InfoView settings.....	779
To change display settings for InfoView.....	779
Managing Web Intelligence settings.....	780
To modify display settings in Web Intelligence.....	781
Managing BI Widgets settings.....	782
Managing Polestar settings.....	782
To modify Polestar application properties.....	782
Chapter 21 Managing Data Sources and Connections	785
Overview.....	786
Data source connections.....	786
Managing universes.....	787
To delete universes.....	787
Managing universe connections.....	787
To delete a universe connection.....	787
Controlling access to universe connections.....	787

Chapter 22	Working with Content Objects	789
	Overview.....	790
	General object management.....	790
	To copy an object.....	790
	To move an object.....	791
	To create an object shortcut.....	791
	Relationships.....	797
	Report object management.....	799
	What are report objects and instances?.....	799
	Setting report refresh options.....	800
	Setting report processing options.....	802
	Processing extensions.....	813
	Applying processing extensions to reports.....	814
	Working with hyperlinked reports	818
	Program object management.....	822
	What are program objects and instances?.....	822
	Setting program processing options.....	824
	Authentication and program objects.....	829
	Object package management.....	832
	What are object packages, components, and instances?.....	832
	Adding objects to an object package.....	833
	Configuring object packages and their objects.....	834
	Authentication and object packages.....	835
Chapter 23	Scheduling Objects	837
	Overview.....	838
	Scheduling.....	838
	About the recurrence options and parameters.....	838
	Scheduling objects using object packages.....	844

Contents

Scheduling an object with events.....	845
Setting general scheduling options.....	847
Setting notification for the success or failure of a scheduling job.....	847
Specifying alert notification.....	851
Selecting a destination.....	853
Choosing a format.....	864
Selecting cache options for Web Intelligence or Desktop Intelligence documents.....	875
Scheduling an object for a user or group.....	876
Selecting server group settings.....	877
Managing instances.....	878
Managing and viewing the history of instances.....	879
Setting instance limits for an object.....	885
Using calendars.....	887
Calendars overview.....	887
Creating calendars.....	887
Adding dates to a calendar.....	888
Deleting calendars.....	893
Specifying calendar rights.....	894
Managing events.....	894
Managing events overview.....	894
File-based events.....	895
Schedule-based events.....	897
Custom events.....	898
Specifying event rights.....	899
To run objects now.....	900

Chapter 24 **Organizing Objects** **901**

Overview.....	902
Organizing objects overview.....	902
About folders	902

Contents

About categories.....	903
Working with folders.....	903
Creating and deleting folders.....	903
Copying and moving folders.....	905
Adding new objects to a folder.....	906
Specifying folder rights.....	907
Setting limits for folders, users, and groups.....	907
Managing Personal Folders.....	909
Working with categories.....	909
Specifying category rights.....	912
 Chapter 25 Adding Objects to the Repository	 913
Overview.....	914
Options for adding Crystal reports.....	914
Publishing Wizard procedures.....	915
Saving objects directly to the CMS.....	929
 Chapter 26 Publishing and Publications	 931
Overview.....	932
About Publishing.....	932
What is a publication?.....	933
Publishing workflow.....	934
Rights required for Publishing.....	935
Publication concepts.....	937
Report bursting.....	937
Delivery rules.....	939
Dynamic recipients.....	942
Destinations.....	943
Formats.....	948
Personalization.....	951

Contents

Subscription.....	952
To create a new publication in the CMC.....	953
To create a new publication in InfoView.....	953
Chapter 27 Managing Profiles	955
How profiles work.....	956
Profiles and the Publishing workflow.....	957
Profile targets and profile values.....	958
To specify a global profile target.....	959
Specifying profile values.....	960
Resolving conflicts between profiles.....	963
Conflicts between profile values.....	964
Specifying profile rights.....	965
Chapter 28 Content Search	967
Content Search overview.....	968
Searchable document types.....	968
Search syntax and interpretation.....	970
Multilingual search.....	972
Content Search and instances.....	973
Facets and labels.....	973
Prompts and Parameters.....	973
Reports with view time security.....	974
Suggested queries.....	975
Limited number of search results.....	976
Excluding documents from Content Search.....	976
Servers and architecture.....	977
Deploying the Content Search service.....	978
Planning your Content Search deployment.....	978
Installation and Upgrade.....	980

Contents

Configuration.....	980
Managing Content Search application settings.....	980
Setting rights for the Content Search application.....	984
Disabling and removing Content Search.....	984
Maximum group instances indexed.....	985
JVM Heap Size.....	986
Understanding and managing the indexing process.....	987
Preparing for the initial indexing.....	987
Creating the initial index.....	988
Managing the indexing program object.....	988
Terminating the indexing process.....	991
Troubleshooting.....	992
To troubleshoot an indexing failure	992
To clean up after unplanned system downtime	993
 Chapter 29 Rights Appendix	 995
About the rights appendix.....	996
General rights.....	996
Rights for specific object types.....	1000
Folder rights.....	1000
Categories.....	1000
Notes.....	1001
Crystal reports.....	1002
Desktop Intelligence documents.....	1003
Web Intelligence documents.....	1004
Users and groups.....	1006
Access levels.....	1007
Dashboards.....	1008
Universes.....	1009
Applications.....	1012

Contents

Chapter 30	Server Properties Appendix	1041
	About the server properties appendix.....	1042
	Common Server Settings.....	1042
	Core Server Settings.....	1044
	Crystal Reports Server Settings.....	1059
	Xcelsius Server Settings.....	1070
	Web Intelligence Server Settings.....	1073
	Web Intelligence Server Memory Threshold Settings	1081
	Desktop Intelligence Server Settings.....	1082
	Voyager Server Settings.....	1091
	Performance Management Server Settings.....	1093
Appendix A	More Information	1095
Index		1099



Getting Started



1

chapter



About this help

This help provides you with information and procedures for deploying and configuring your BusinessObjects Enterprise system. Procedures are provided for common tasks. Conceptual information and technical details are provided for all advanced topics.

For daily maintenance tasks and procedures for working with the CMC, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

For information about installing BusinessObjects Enterprise, see the *SAP BusinessObjects Enterprise Installation Guide*.

Who should use this help?

This help covers deployment and configuration tasks. We recommend consulting this guide if you are:

- planning your first deployment
- configuring your first deployment
- making significant changes to the architecture of an existing deployment
- improving your system's performance.

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

About BusinessObjects Enterprise

BusinessObjects Enterprise is a flexible, scalable, and reliable solution for delivering powerful, interactive reports to end users via any web application—intranet, extranet, Internet or corporate portal. Whether it is used for distributing weekly sales reports, providing customers with

personalized service offerings, or integrating critical information into corporate portals, BusinessObjects Enterprise delivers tangible benefits that extend across and beyond the organization. As an integrated suite for reporting, analysis, and information delivery, BusinessObjects Enterprise provides a solution for increasing end-user productivity and reducing administrative efforts.

What's new in BusinessObjects Enterprise XI 3.1?

This version of BusinessObjects Enterprise introduces many new features and enhancements. The following table briefly describes these features and where to find more information about them.

What's New	Documentation resources
Server management: Server management is now handled through the CMC and the Server Intelligence Agent (SIA).	<ul style="list-style-type: none"> • About Server Intelligence • Server management: what's new in this version of BusinessObjects Enterprise
Federation: This cross-site replication tool allows you to manage content from a BusinessObjects Enterprise deployment (Origin site) and replicate it to other BusinessObjects Enterprise deployments (Destination sites).	<ul style="list-style-type: none"> • Federation
Publishing: This version features user interface improvements to the Publishing feature. Also, all report bursting methods are now supported for Web Intelligence document publications.	<ul style="list-style-type: none"> • About Publishing • For more information, see the <i>SAP BusinessObjects Enterprise Publisher's Guide</i>. The latest version of the PDF is available on the Business Objects technical support site.

What's New	Documentation resources
Instance Manager: In this release, the Instance Manager shows more details for listed instances.	<ul style="list-style-type: none"> • Instance Manager • Managing instances
Web Application Container Server (WACS): The WACS is a service that hosts the CMC for users that are installing BusinessObjects Enterprise on a Windows environment and don't want to deploy the CMC to a Java application server.	<ul style="list-style-type: none"> • Web Application Container Server (WACS)
Windows Active Directory authentication: Multi-forest support is integrated into the process of using the CMC to set up AD authentication with either the Kerberos or NTLM protocols.	<ul style="list-style-type: none"> • Scheduling AD updates
Server settings: BusinessObjects servers now support IPv6.	<ul style="list-style-type: none"> • Network environment options
Reverse proxy: Microsoft ISA 2006 is now supported as a reverse proxy server.	<ul style="list-style-type: none"> • To configure Microsoft ISA 2006 for BusinessObjects Enterprise

Online documentation library

A completely new interface to the full documentation set now has guides for all Business Objects products. The new online documentation library has the most up-to-date version of the Business Objects product documentation, posted upon publication and updated regularly. You can browse the library contents, run full-text searches, read guides on line, and download PDFs.

http://support.businessobjects.com/documentation/product_guides/default.asp

Where should I start?

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

- [Planning or performing your first deployment](#)
- [Configuring your deployment](#)
- [Changing your deployment's architecture](#)
- [Improving your system's performance](#)
- [Working with objects in the CMC](#)

Planning or performing your first deployment

If you are planning or performing your first deployment of BusinessObjects Enterprise, it is recommended that you perform the following tasks and read the corresponding sections:

- To get familiar with the components, read [Architecture overview](#).
- To assess your needs and design a deployment architecture that works best for you, read the *SAP BusinessObjects Enterprise Planning Guide*.
- [Understanding communication between BusinessObjects Enterprise components](#)
- [Security overview](#)
- If you plan to use third-party authentication, read [Configuring Third-Party Authentication](#)
- For advice about assessing your anticipated performance needs, see [Improving performance](#).
- For more information about installing BusinessObjects Enterprise, see the *SAP BusinessObjects Enterprise Installation Guide*.
- After you install, read [Server management overview](#).

Configuring your deployment

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

- [Server management overview](#)
- [Understanding communication between BusinessObjects Enterprise components](#)
- [Security overview](#)
- If you plan to use third-party authentication, read [Configuring Third-Party Authentication](#)
- For advice about assessing and improving your system's performance, see [Improving performance](#).
- If you want to monitor your existing system, read [Managing Auditing](#) and [Auditing Reports](#).

Changing your deployment's architecture

Are you expecting a significant increase in server traffic? Do you need to accommodate a sudden influx of users? Do you need to incorporate new kinds of content from new sources? Or do you need to update a deployment that didn't adequately anticipate the volume of objects being processed on a daily basis?

If you need to revise your deployment to account for significant changes in how you use the system, it is recommended that you read the following sections:

- For advice about assessing and improving your system's performance, see [Improving performance](#).
- If you are installing new server components, see [Server management overview](#).
- If you are importing or configuring new users, see [Account management overview](#).

- For information about installing new components, you can find more information in the *SAP BusinessObjects Enterprise Installation Guide*.

Improving your system's performance

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

- For advice about assessing and improving your system's performance, see [Improving performance](#).
- If you want to monitor your existing system, read [Managing Auditing](#) and [Auditing Reports](#).
- For daily maintenance tasks and procedures for working with servers in the CMC, see [Server management overview](#).

Working with objects in the CMC

If you are working with objects in the CMC, read the following sections:

- To get started with the CMC, see [Using the CMC](#).
- For information about setting up users and groups in the CMC, see [Account management overview](#).
- To add objects to BusinessObjects Enterprise, see [Overview](#).
- To set security on objects, see [How rights work in BusinessObjects Enterprise](#).
- For general information about working with objects, see [General object management](#).
- To organize objects, see [Organizing objects overview](#).
- To schedule objects in BusinessObjects Enterprise, see [Scheduling](#).

SAP BusinessObjects Enterprise guides

The following table provides a list of SAP BusinessObjects Enterprise guides and their contents.

Guide	Description
SAP BusinessObjects Enterprise Planning Guide	Covers the key concepts you should consider before you begin deploying SAP BusinessObjects Enterprise. This guide includes an overview of the architecture, tips for assessing your existing environment, determining your organization's needs, and preparing for the installation.
SAP BusinessObjects Enterprise Installation Guide	Leads you through the steps required to run the setup program and complete your installation of SAP BusinessObjects Enterprise. There are UNIX and Windows versions of this guide available.
SAP BusinessObjects Enterprise Web Application Deployment Guide	Covers topics related to the deployment of web applications to web application servers with SAP BusinessObjects Enterprise. There are UNIX and Windows versions of this guide available.
SAP BusinessObjects Enterprise Administrator's Guide	Provides content for server and content administration. The server administration topics includes server configuration, managing authentication, configuring firewalls, and measuring system performance. The content administration topics include working with the CMC, configuring rights and access levels, managing users, and working with Business Objects applications and objects.

Guide	Description
SAP BusinessObjects Enterprise Publisher's Guide	Provides an overview of the publishing process, working with publications, publishing Crystal reports, publishing Web Intelligence documents, publishing Desktop Intelligence documents, and publishing security.
SAP BusinessObjects 5/6 to XI 3.1 Migration Guide	Details content migration from legacy Business Objects software, such as Classic or Enterprise 5 or 6, to SAP BusinessObjects Enterprise XI 3.1.
SAP BusinessObjects Enterprise Upgrade Guide	Information for upgrades from BusinessObjects Enterprise XI to SAP BusinessObjects Enterprise XI 3.1.
SAP BusinessObjects Enterprise InfoView User's Guide	Provides an overview of InfoView and working with Crystal Reports, Web Intelligence, objects, discussions, encyclopedia, and Voyager workspaces.

For a complete list of all of our product documentation please visit:
http://support.businessobjects.com/documentation/product_guides/default.asp



Architecture



2
chapter



Architecture overview

This section outlines the overall platform architecture, system, and service components that make up the BusinessObjects Enterprise Business Intelligence (BI) platform. This information will help administrators understand the system essentials, and help to form a plan for the deployment, management, and maintenance of an BusinessObjects Enterprise installation.

Business Intelligence is the process of taking raw data stored in databases, and turning it into useful information in the form of reports that can be used to make business decisions. BI reports can be used internally and externally throughout an organization to make tactical decisions, reduce costs, streamline operations, build better products, increase sales, or deepen customer relationships.

BusinessObjects Enterprise includes specialized services including Web Intelligence, Desktop Intelligence, and Crystal Reports components, and a set of Dashboard and Analytics services for metrics management, predictive analysis, and process analysis. These services are available to software created by your own organization through several application programming interfaces (APIs).

BusinessObjects Enterprise is designed for high performance across a broad spectrum of user and deployment scenarios. For example, specialized platform services handle either on-demand data access and report generation, or report scheduling based on times and events. You can offload processor intensive scheduling and processing to dedicated servers to improve performance. The architecture is designed to meet the needs of virtually any BI deployment, and is flexible enough to grow from several users with a single tool, to tens of thousands of users with multiple tools and interfaces.

Developers can access the platform using a set of web services and Java and .NET APIs to integrate BusinessObjects Enterprise into your organization's systems, and to share dynamically updated documents with users on separate networks.

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

- Crystal Reports.
- Web Intelligence.
- Desktop Intelligence.
- Voyager.

- Dashboard and Analytics.
- Dashboard Builder.

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

- Central Management Console.
- Central Configuration Manager.
- Import Wizard.
- Publishing Wizard.
- Universe Designer.
- Repository Diagnostic Tool.

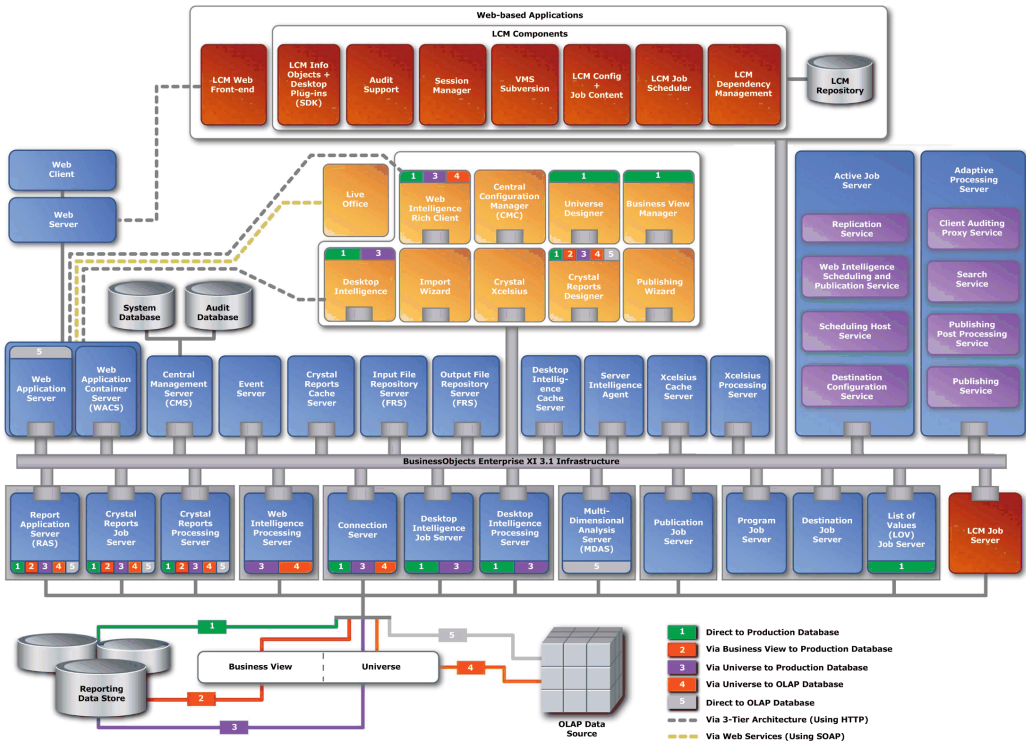
To provide flexibility, reliability, and scalability, the components that make up BusinessObjects Enterprise can be installed on one or many machines. You can even install two BusinessObjects Enterprise deployments simultaneously on the same hardware, although this configuration is recommended only for upgrade or testing purposes.

Server processes can be “vertically scaled” (where one computer runs several, or all, server-side processes) to reduce cost, or “horizontally scaled” (where server processes are distributed between two or more networked machines) to improve performance. It is also possible to run duplicate instances of a server process on the same machine, or across several networked machines.

Note:

While it is possible to deploy a mixture of Windows and Unix platforms at the tier level (such as a Unix web application server with a Windows CMS), it is recommended that you do not mix operating systems for server processes (such as a cluster of two CMS systems where one runs Windows and the other runs Unix).

Enterprise infrastructure



The Enterprise Infrastructure provides the basic messaging mechanism needed for BusinessObjects Enterprise components to communicate with one another. The Enterprise Infrastructure is a series of services that are designed to communicate via CORBA (Common Object Request Broker Architecture), which runs over TCP/IP.

Some CORBA applications use a name server. The name server service is a facility of the underlying CORBA architecture that binds the BusinessObjects Enterprise servers together. The name server provides a directory of the servers registered in the BusinessObjects Enterprise environment and helps establish connections between clients and these servers. The name server service is a part of the Central Management Server (CMS).

The Enterprise Infrastructure provides the framework for establishing connections between clients and servers:

- It is the centerpiece of BusinessObjects Enterprise technology, and facilitates communication between servers.
- A client object can transparently make requests to server objects using the Enterprise Infrastructure.
 - A server object is a server that participates in serving requests to client objects.
 - A client object is a client that makes requests to servers on the Enterprise Infrastructure.

Note:

In the BusinessObjects Enterprise environment, most services act as clients and servers to each other during transactions between the servers.

When a BusinessObjects Enterprise server starts, it registers itself with the name server in the CMS. The server provides information about itself, such as its IP address, TCP port, and description of the server, and a list of services it provides, to the name server.

Each individual server polls the CMS every 60 seconds to get an updated list of provided services.

BusinessObjects Enterprise web services

The web services are server-side components that process requests from client applications and communicate these requests to the appropriate server. They include support for report viewing, and logic to understand and direct web requests to the appropriate BusinessObjects Enterprise server.

BusinessObjects Enterprise web services are hosted on the web application server. Web services use the BusinessObjects Enterprise SDK to interface with the rest of the BusinessObjects Enterprise services. The web application server acts as a gateway between the browser and the rest of the components in BusinessObjects Enterprise.

Note:

When configuring servers using the Central Management Console, the CMS holds the configuration settings and the CMS communicates with all BusinessObjects Enterprise servers.

Business Objects web services provide a Java and .NET consumers API accessed by rich clients in the user interaction tier, such as Live Office and Crystal Reports.

Web Services consists of software components that can be called remotely using the Simple Object Access Protocol (SOAP). SOAP is a protocol for exchanging information that is not dependent on a specific platform, object model, or programming language.

BusinessObjects Enterprise Web Services provide services in the following areas:

- Session: Authentication and user privilege management.
- BI platform: Exposes advanced platform features such as scheduling, search, user and group administration, server administration, platform events, and calendars.
- Report Engine: Displays Web Intelligence and Crystal Reports in HTML, PDF, Excel, and XML format.
- Query: Builds ad hoc queries based on the Business Objects universe semantic layer.

Web application clustering support

The Central Management Console (CMC) and InfoView web applications can be used in environments with a variety of different clustered, load balanced, or fault tolerant configurations. The table below lists configuration support for CMC and InfoView web applications.

Web application	Clustered web application servers	Load balancers with session affinity	Load balancers without session affinity	Fault tolerant
InfoView (stateless)	Supported	Supported	Supported	Yes
CMC (stateful)	Supported	Supported	Unsupported	No

BusinessObjects Enterprise management services

The management services manage the BusinessObjects Enterprise system. These services maintain all security information, send requests to the appropriate services, manage auditing information, and maintain a record of each and every instance and its location.

The management services are provided by:

- Central Management Service running on the Central Management Server (CMS)

The CMS is responsible for authenticating users and groups, and keeping track of the availability of the other BusinessObjects Enterprise services. It also maintains the BusinessObjects Enterprise system database, which includes information about users, groups, security levels, BusinessObjects Enterprise content, and services. The CMS also maintains a separate audit database of information about user actions and manages the BusinessObjects system database.

Note:

- All servers communicate with the CMS when they start up.
- The Audit Database is optional in a regular system deployment. It allows for extra auditing and tracking of some system information.
- Event Service running on the Event Server

The Event Server manages file-based events. It monitors the directory you specified when setting up a file-based event. When the appropriate file appears in the monitored directory, the Event Server triggers a file-based event.

BusinessObjects Enterprise storage services

The storage services are responsible for storing objects and object instances.

The storage services are:

- Input File Repository Service running on the Input File Repository Server

The Input File Repository Service manages all of the report and program objects that have been published to the system. It can store the following files: `.rpt`, `.car`, `.exe`, `.bat`, `.js`, `.xls`, `.doc`, `.ppt`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`, or `.unv`.

- Output File Repository Service running on the Output File Repository Server

The Output File Repository Service manages all of the report instances generated by the Crystal Reports Job Service and the program instances generated by the Program Job Service. It also manages instances generated by the Desktop or Web Intelligence Processing Services, and the List of Values (LOV) Job Service.

It can store the following files: `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, or `.rep`.

Note:

`.rpt` and `.wid` files are stored as report documents with saved data.

- Crystal Reports Cache Service running on the Crystal Reports Cache Server

The Crystal Reports Cache Service maintains a folder of cached report EPF files and determines if a request can be fulfilled with a cached report page. If the request cannot be fulfilled with a cached report page, it passes the request to the Crystal Reports Processing Service.

The benefit of caching is that BusinessObjects Enterprise doesn't have to generate `.epf` files each time a page is viewed. Therefore, report pages that have been cached can be shared among users.

- Desktop Intelligence Cache Service running on the Desktop Intelligence Cache Server

The Desktop Intelligence Cache Service handles viewing requests for Desktop Intelligence documents and manages the viewable pages created by the Desktop Intelligence Processing Service.

BusinessObjects Enterprise processing services

The processing services access the data and generate reports. This is the only tier that interacts directly with the databases that contain report data.

Which services become involved with reporting is determined by whether the object is being scheduled or viewed on demand. Viewer choice also plays a role in determining which services and servers are involved in reporting.

The processing services are:

- Program Job Service running on the Program Job Server

The Program Job Service processes program objects, as requested by the CMS, and generates program instances.

- Crystal Reports Job Service running on the Crystal Reports Job Server

The Crystal Reports Job Service schedules and processes report objects, creating report instances at the request of the Central Management Server (CMS).

Note:

Both the Program Job Service and the Crystal Reports Job Service retrieve the document to be run from the Input File Repository Service, run the report or program, and then save the processed file to the Output File Repository Service as an instance.

- Web Intelligence Job Service running on the Adaptive Job Server

The Web Intelligence Job Service receives scheduled Web Intelligence document requests from the CMS and forwards them to the Web Intelligence server for processing.

Note:

It is not the Adaptive Job Server itself that processes Web Intelligence documents, but rather the Web Intelligence Job Service hosted by the Adaptive Job Server (AJS). The AJS can be configured to run with or without the Web Intelligence Job Service.

- Web Intelligence Processing Service running on the Web Intelligence Processing Server

The Web Intelligence Processing Service processes Web Intelligence Document requests.

- List of Values (LOV) Job Service running on the LOV Job Server

The List of Values Job Service receives scheduling requests from the Business View manager and processes scheduled List of Values objects to populate them with values retrieved from a database.

- Desktop Intelligence Job Service running on the Desktop Intelligence Job Server

The Desktop Intelligence Job Service processes scheduling requests received from the CMS for Desktop Intelligence documents and generates instances of the Desktop Intelligence document.

- Desktop Intelligence Processing Service running on the Desktop Intelligence Processing Server

The Desktop Intelligence Processing Service processes viewing requests for Desktop Intelligence documents, generating Desktop Intelligence documents.

- Connection Service running on the Connection Server

The Connection Service is responsible for the database connectivity to access data. It is invoked when users want to edit and view Desktop or Web Intelligence documents through InfoView. It is also used by some EPM services.

Note:

The Connection Service libraries are present on the Web Intelligence Processing Server, and Desktop Intelligence Processing Server. These libraries allow services to query the database directly without communicating with the Connection Server service.

- Publishing Post Processing Service running on the Adaptive Processing Server

This service is responsible for any post processing of a publication job, including PDF merging and publication extension processing.

- Web Application Container Service (WACS)

The Web Application Container Service (WACS) provides a platform for hosting BusinessObjects Enterprise web applications, such as the Central Management Console (CMC).

Web applications such as the CMC are automatically deployed to WACS. WACS does not support deploying Business Objects or external web applications, whether manually or by using the wdeploy tool.

The viewing processing services are:

- Crystal Reports Processing Service running on the Crystal Reports Processing Server

The Crystal Reports Processing Service is responsible for generating Crystal Reports pages for viewing. The Crystal Reports Processing Service retrieves data for the report from the latest instance or directly from a database. After it generates the report, the Processing Service converts the requested data to one or more EPF files. These files are then sent to the Crystal Reports Cache Service.

- Web Intelligence Processing Service running on the Web Intelligence Processing Server

The Web Intelligence Processing Service is responsible for generating Web Intelligence documents. The Web Intelligence Processing Service obtains document creation requests from the web application server and then communicates with the Input File Repository Service in order to obtain a copy of the Web Intelligence Document (WID) file and the universe definition. When viewing an existing instance of a WID, the Web Intelligence Processing Service communicates with the Output File Repository Service to obtain an existing historical instance of a WID.

- Report Application Service running on the Report Application Server

Report Application Service resolves Dynamic Recipient Lists at design time and Runtime in Publishing, as well as with LiveOffice. The RAS also provides the ad hoc reporting capabilities that allow users to create and modify reports over the Web.

As with the Crystal Reports Processing Service, the RAS supports Java viewer SDKs. The Report Application Service also includes an SDK for report creation and modification, providing you with tools for building custom report interaction interfaces.

- Multi-Dimensional Analysis Service running on the Multi-Dimensional Analysis Server

The Multi-Dimensional Analysis Server (MDAS) is a dedicated server intended to interact with OLAP data sources and to support Voyager.

The MDAS needs an appropriate OLAP database client configured for the appropriate OLAP data source. The list of providers is dynamically generated, based on which database drivers are installed on the MDAS. If more than one MDAS exists, the server contacted is selected randomly, so the same drivers should be installed on all servers. Connections to OLAP data sources are defined and managed from the CMC. Entries can include:

- Oracle
 - SAP
 - Essbase
 - Microsoft Analysis Services 8.0 (MSAS 2000)
 - Microsoft Analysis Services 9.0 (MSAS 2005)
- Search Service running on the Adaptive Processing Server

The Search Service processes search requests and executes the indexing. Your deployment can include multiple Search service, and search requests are actively processed by all available servers. However, only one Search service performs the indexing process.

- Client Auditing Proxy Service running on the Adaptive Processing Server

The Client Auditing Proxy Service monitors connected Rich Web Intelligence and Rich Desktop Intelligence clients and forwards the information to the auditing server. Rich clients working locally, not connected to a repository, are not audited by the Client Auditing Proxy Service.

- Publishing Service running on the Adaptive Processing Server

The Publishing Service coordinates the publication of an object by communicating with other services to process the publication.

Server Intelligence

Server Intelligence is a component of the Central Management Console (CMC) that simplifies administrative procedures previously carried out by the Central Configuration Manager (CCM), such as the management of CMC server processes. This includes the addition and removal of server processes,

server process configuration, and the automatic restart or shutdown of servers that encounter unexpected conditions.

Server Intelligence also archives server process information in the CMS database so you can easily restore default server settings, or create redundant instances of server processes with the same settings.

Note:

The CCM is a tool that allows you to configure and manage the Server Intelligence Agent. The Server Intelligence Agent is the component that allows you to manage all servers through the CMC. You can also use the CCM to create and manage nodes in your deployment.

Life-Cycle Management (LCM)

BusinessObjects Enterprise contains new Life-Cycle Management modules that gives you control over your life cycles of system objects.

Life-Cycle Management refers to the set of processes involved in managing information related to a product life cycle, from the stage of concept through delivery. It establishes procedures for governing the entire product life cycle, which includes phases such as development, production, testing, and so on.

The BI resources that are present in the development repository must be transferred to the testing repository for testing deployment. These phases can occur at the same site or at different geographical locations. The time required to transfer the resources from one repository to another repository must be minimal, to obtain a high-quality and competitive product. These resources also have dependencies that have to be moved from one repository to another. The dependencies of resources add more complexity to the problem, because these resources have to move along with the dependents.

For more information, see the *SAP BusinessObjects Enterprise Life-Cycle Manager User's Guide for XI 3.1*.

Life-Cycle Manager

BusinessObjects LifeCycle Manager (LCM) is a web-based tool that enables you to move BI resources from one system to another system, without affecting the dependencies of these resources. It also enables you to manage

different versions of BI resources, manage dependencies of BI resources, and roll back a promoted resource to restore the destination system to its previous state.

The LCM tool is a plug-in for the BusinessObjects Enterprise application. You can promote a BI resource from one system to another system only if the same version of the BusinessObjects Enterprise application is installed on both the source and destination systems.

Clients

Two different types of applications are available: web browser clients, and rich desktop application clients installed on a Microsoft Windows operating system.

Browser-based web applications

This category is made up of light-weight, web browser-based client front-ends that run on all supported operating system platforms. A web application server receives client requests and interfaces with the BusinessObjects Enterprise intelligence and processing tiers to return data to the users' web browsers. This approach allows you to provide business intelligence (BI) access to large groups of users, without the challenges of deploying desktop software products. Communication is conducted over HTTP and can be secured with SSL by enabling HTTPS encryption on the web application server. Examples of this type of application include the InfoView, Web Intelligence, Central Management Console (CMC), and report viewers.

Desktop applications

The second category is made up of locally installed, rich-client applications installed on a supported Microsoft Windows operating system. This approach allows you to offload BI processing from BusinessObjects Enterprise onto individual client computers. Most desktop applications directly access your organization's data through drivers installed on the desktop, and communicate with your BusinessObjects Enterprise deployment through CORBA or encrypted CORBA SSL. Examples of this type of application include Crystal Reports, Desktop Intelligence, and Live Office clients.

Note:

Although Live Office is a desktop application, it communicates with BusinessObjects Enterprise web services over HTTP. You can configure BusinessObjects Enterprise so that Microsoft Office documents containing Live Office components dynamically update, even when sent to recipients outside your organization's secured network.

Browser-based web application clients

Browser-based web application clients reside on a web application server, and run in a web browser.

Web applications are automatically deployed by the setup program when you install BusinessObjects Enterprise. Java web applications can also be reconfigured or deployed after the initial installation using the bundled `wdeploy` command-line tool. The `wdeploy` tool is designed to speed up and simplify deployment to Java web application servers. Based on the Apache Ant scripting tool, `wdeploy` allows you to deploy WAR files to a web application server in two ways:

1. Standalone mode.

All web application resources are deployed together on a web application server that serves both dynamic and static content.

2. Split mode.

The application's dynamic and static resources are separated: static content is deployed to a web server; dynamic content is deployed to a web application server.

For more information about `wdeploy`, see the BusinessObjects Enterprise Web Application Deployment Guide.

BusinessObjects Mobile

BusinessObjects Mobile allows your organization access to information from any wireless device. Management and information workers can stay up-to-date and make decisions with access to the latest information. Sales and field service staff can provide the right customer, product, and work order

information, where and when it's needed, helping to shorten sales cycles, and increasing customer satisfaction.

Central Management Console (CMC)

The Central Management Console (CMC) is a web-based tool to perform regular administrative tasks, including user, content, and server management. It also allows you to publish, organize, and set security levels for all of your BusinessObjects Enterprise content. Because the CMC is a web-based application, you can perform all of these administrative tasks through a web browser on any machine that can connect to the server.

All users can log on to the CMC to change their user preference settings. Only members of the *Administrators* group can change management settings, unless explicitly granted the rights to do so.

Dashboard and Analytics

Dashboard and Analytics is a suite of products that helps users track and analyze key business metrics via management dashboards, scorecards, and alerting. These products allow goals to be set around metrics and assigned to owners; they also support group decision-making and analysis via integrated collaboration and workflow capabilities.

Dashboard and Analytics includes the following products:

- Dashboard Builder
- Performance Manager
- Set Analysis
- Predictive Analysis
- Process Analysis

The Dashboard and Analytics repository stores the metrics, goals, sets and calendar definitions, used by Dashboard and Analytics users to create dashboards and analytics. Each time users refresh a metric, the values for the metric refresh are written to the Dashboard and Analytics repository.

Note:

To use Dashboard and Analytics features, you must purchase a BusinessObjects Enterprise license that includes the use of Dashboard and Analytics as part of its agreement.

BusinessObjects Enterprise InfoView

InfoView is a web-based interface that end users access to view, schedule, and keep track of published reports. InfoView can access, interact with, and export, any type of business intelligence including reports, analytics, dashboards, scorecards, and strategy maps.

InfoView allows users to manage:

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

Report viewers

BusinessObjects Enterprise includes report viewers that support different platforms and different browsers in the client tier, and which have different report viewing functionality.

Report viewers fall into two categories:

- Client-side report viewers (Active X viewer, Java viewer)

Client-side report viewers are downloaded and installed in the user's browser. When a user requests a report, the application server processes the request, and retrieves the report pages from the BusinessObjects Enterprise framework. The web application server then passes the report pages to the client-side viewer, which processes the report pages and displays them directly in the browser.

- Zero-client report viewers (DHTML viewer)

Zero-client report viewers reside on the web application server. When a user requests a report, the web application server processes the request, and then retrieves the report pages from the BusinessObjects Enterprise framework. The web application server processes the report and creates DHTML pages that the viewer displays in the user's web browser.

All report viewers help process requests for reports, and present report pages that appear in the user's browser.

For more information on the specific functionality or platform support provided by each report viewer, see the *BusinessObjects Enterprise InfoView User's Guide* or the *Crystal Reports Developer's Guide*, available at the customer support portal: http://support.businessobjects.com/documentation/product_guides/default.asp.

Voyager

Voyager is an AJAX-based online analytical processing (OLAP) tool for working with multi-dimensional data, combining information from different systems within a single workspace. Users access Voyager from within the BusinessObjects Enterprise InfoView portal. Users can create new analysis workspaces, and view and edit workspaces that have been saved to the BusinessObjects Enterprise repository.

Voyager is accessed from BusinessObjects InfoView in a web browser, which can be distributed to a large number of users, including those outside of your secure network, on the internet.

The Voyager OLAP feature set complements both Crystal Reports (for direct data access to OLAP cubes for production reporting) and Web Intelligence (for ad hoc analytic reporting with universes built on OLAP data sources). Voyager offers a comprehensive range of business and time calculations, and includes features such as time sliders to make the analysis of OLAP data as simple as possible.

Voyager requires a connection to a supported OLAP data source, such as Microsoft Analysis Services, SAP BW, or Oracle Hyperion Essbase. Therefore, you must create a connection to data before analysts can begin using Voyager to analyze data.

Note:

The Voyager web application is available only as a Java web application. There is no corresponding Voyager application for .NET.

Web Intelligence

A web-based tool that provides query, reporting, and analysis functionality for relational data sources in a single web-based product. Web Intelligence allows users to create reports, perform ad hoc queries, analyze data, and apply report formatting in a drag-and-drop interface. Web Intelligence hides the complexity of underlying data sources. Reports can be published to the BusinessObjects Enterprise web portal, or to Microsoft Office applications using BusinessObjects Live Office.

Desktop client applications

Desktop client applications interact with the BusinessObjects Enterprise intelligence or processing servers. They do not communicate with the web application server. Communication between the clients and the servers can be secured with SSL encryption (CORBA SSL).

Desktop products are installed client applications that run on Microsoft Windows operating systems. They can store resources locally and access your organization's data through locally installed database driver or the Central Management Console (CMC).

Business View Manager

A Windows-based tool that allows users to build semantic layer objects that simplify underlying database complexity, and set row- and column-level security. It is a multi-tier system that enables companies to build comprehensive and specific Business View objects that help report designers and end-users access the information they require.

The objects (such as filters) set row-level security. You can simplify data access for report designers by insulating them from the raw data structures. You can build connections to multiple data sources, join tables, alias field names, create calculated fields, and then utilize this simplified structure as a Business View in BusinessObjects Enterprise. Report designers can then use the Business View as the basis for their reports, rather than accessing the data directly and building their own queries.

This designer provides a wide range of capabilities for creating Data Connections, Dynamic Data Connections, Data Foundations, Business Elements, and Business Views. The Business View Manager allows you to design relational views of information. This designer also allows you to set detailed column and row-level security for various objects in a report.

Central Configuration Manager (CCM)

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

The CCM allows you to create and configure Server Intelligence Agent (SIA) nodes and start or stop your web application server. On Windows, it also allows you to configure network parameters, such as Secure Socket Layer (SSL) encryption. These parameters apply to all servers within a node.

Note:

Most server management tasks are now handled through the CMC, not through the CCM. The CCM was the primary tool for server management in previous versions of BusinessObjects Enterprise, but the CCM is now used for troubleshooting and node configuration.

Crystal Reports Designer

Crystal Reports Designer allows database experts or application developers to create and integrate detailed reports that can be easily shared with others using Crystal Reports Viewer or a web browser.

Crystal Reports Viewer

The Crystal Reports Viewer is available as a free download from <http://www.businessobjects.com/product/catalog/crystalreports>, and allows users to open reports in read-only mode. Reports cannot be refreshed, as the data used is saved within the report itself.

Data Source Migration Wizard

The Data Source Migration Wizard allows you to migrate reports that are based on Crystal Reports queries, dictionaries, or InfoViews, to a BusinessObjects Enterprise deployment.

You can migrate two types of objects: reports and data sources. The wizard converts the data source of each report into an object that is usable in BusinessObjects Enterprise, and then resets the data source location of the report to point to the new object. The result is that you can use the new features of BusinessObjects Enterprise while keeping the functionality of the reports and data sources from your previous installation.

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.

Desktop Intelligence

A Windows-based integrated query, reporting and analysis tool that allows you to access data using familiar business terms, rather than using technical database query methods, like SQL. The complexity of the underlying data storage is abstracted in the semantic data layer known as the Business Objects Universe.

Designers can create reports, then publish them to InfoView, where they can be viewed and scheduled. Users can share and distribute Desktop Intelligence documents by exporting them in different formats.

Import Wizard

A locally-installed Windows application that guides administrators through the process of importing users, groups, and folders into BusinessObjects Enterprise. It also allows you to import objects, events, server groups, repository objects, and calendars in BusinessObjects Enterprise.

Live Office

BusinessObjects Live Office integrates with the Microsoft Office environment, allowing for dynamically updated data to be embedded within Microsoft Outlook, PowerPoint, Excel, and Word documents. Plus, you can share your documents with others over the web for collaborative decision-making. From within Microsoft Office, you can use intuitive wizards and toolbars to easily connect to a Crystal report, Web Intelligence document, or use ad hoc data selections. Then format your data using familiar Microsoft Office tools.

Using Live Office, you can publish "live" documents to BusinessObjects Enterprise for sharing with your coworkers through a business intelligence portal. Or, take it outside the firewall and e-mail it to an off-site partner or coworker.

Note:

Web services applications are currently only supported with the following load balancer configurations:

1. Source IP address persistence.
2. Source IP and destination port persistence (available only on a Cisco Content Services Switch).
3. SSL persistence.

Note:

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

For information on configuring web services to work with Live Office, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Publishing Wizard

The Publishing Wizard enables both administrators and end users to publish reports to BusinessObjects Enterprise. By assigning object rights to individual folders on a given server, you control who can publish reports and where they are published.

Use the Publishing Wizard if you have access to the application and you want to add multiple objects or an entire directory of objects to

BusinessObjects Enterprise. Once an object is added, it appears in the folder that you specified in InfoView (or your customized web desktop) and in the **Folders** management area of the CMC.

For more information, see the *Adding Objects to the Repository* chapter of *SAP BusinessObjects Enterprise Administrator's Guide*.

Query as a Web Service (QaaWS)

Query as a Web Service provides new and easy ways to analyze information through user-driven client solutions for businesses. Business Intelligence (BI) content is usually bound to a specific user interface of BI tools. Query as a Web Service changes this by allowing BI content to be delivered to any user interface that can process web services.

Using Query as a Web Service, business users define their own query from a universe, and then easily and securely publish that query as a standalone web service.

Query as a Web Service provides new client solutions for businesses. For example, it enables Crystal Xcelsius to aggregate multiple disparate data sources into a trusted BI view.

Query as a Web Service also enables a range of client-side solutions in tools such as:

- Microsoft Office, Excel, and InfoPath.
- SAP Application Server.
- OpenOffice.
- Business rules and process management applications.
- Enterprise Services.

Report Conversion Tool

The Report Conversion Tool converts Desktop Intelligence reports to the Web Intelligence format and publishes the converted reports to the CMS.

It retrieves reports from the CMS, in the Public, Favorites, or Inbox folders. Once converted, you can publish to the same folder as the original Desktop Intelligence report or to a different folder. The tool does not convert all Desktop Intelligence features and reports. The level of conversion depends

on the features in the original report. Some features prevent the report from being converted. Other features are modified, reimplemented, or removed by the tool during conversion.

The tool assigns one of three statuses to each report:

- Fully Converted.
- Partly Converted.
- Not Converted.

The Report Conversion Tool also lets you audit your converted reports. This helps identify reports that cannot be fully converted by the Report Conversion Tool and explains why.

Repository Diagnostic Tool

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

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

Translation Manager

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

The Translation Manager is the tool that defines the multilingual universes and manages translation of universes and their Web Intelligence documents and prompts.

Translation Manager:

- Translates universe or a Web Intelligence documents for a multilingual audience.
- Defines the metadata language parts of the document and the appropriate translation. It generates external XLIFF format and imports XLIFF files to get translated information.
- Lists the universe or Web Intelligence document structure to be translated.
- Lets you translate the metadata through the interface.
- Lets you translate the metadata using external translation tools by exporting and importing XLIFF files.
- Creates a multilingual document where several languages can be saved.

Universe Builder

A universe is a semantic layer of abstraction that exists between BusinessObjects Enterprise and the data in your organization's database. Universe Builder allows you to create universes from XML metadata and Oracle Analytic Services.

Universe data sources can be multi-dimensional objects (dimensions, measures, details), enabling the end user to analyze the data without needing to know the details of the underlying database structure.

Once you start Universe Builder, you connect to a metadata source, then using a universe creation wizard, map metadata structures to equivalent classes, objects, dimensions, and details, used in a standard BusinessObjects universe.

You can create universes from metadata sources with both Universe Builder and Designer. Universe Builder is a stand-alone product that provides an independent user interface for universe creation from metadata sources. Designer is used for the universe generation at the end of the creation process.

Universe Designer

Universe Designer provides a connection wizard that allows you to connect to your database. You can create multiple connections with Universe Designer, but only one connection can be defined for each universe. This database connection is saved with the universe.

The objects (such as filters) set row-level security. This semantic layer is the foundation for empowering end users to customize query and analysis. It abstracts the complexity of data by using business language rather than data language to access, manipulate, and organize data.

Universe Designer provides a graphical interface to select and view tables in a database. The database tables are represented as table symbols in a schema diagram. You can use this interface to manipulate tables, create joins between tables, create alias tables, create contexts, and solve loops in your schema. Web Intelligence users do not see this schema.

Web Intelligence Rich Client

Web Intelligence Rich Client allows you to continue to work with Web Intelligence documents (WID) when you are unable to connect to a CMS, when you want to perform calculations locally rather than on the server, or when you want to work with Web Intelligence documents without installing a CMS or application server.

Web Intelligence Rich Client can also be used when connected to a CMS.

Xcelsius

Xcelsius is a data visualization tool that transforms BI data into engaging presentations and dashboards. It enables the integration of dynamically updated data into Microsoft Office, PDF, and web documents with Business Objects queries and reports. Xcelsius is comprised of designer and viewing extensions leveraging Business Objects web services.

Services

BusinessObjects Enterprise uses the terms *server* and *service* to refer to the two types of software running on a BusinessObjects Enterprise machine.

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

While the term *server* can refer to a physical machine on which a software system is running, it is also used to describe an operating system level process (or *daemon*) hosting one or more services. For example, the Central Management Server (CMS) and Adaptive Processing Server are servers. A server runs under a specific operating system account and has its own PID.

A *node* is a collection of BusinessObjects Enterprise servers running on the same host. One or more nodes can be on a single host.

BusinessObjects Enterprise can be installed on a single machine, spread across different machines on an intranet, or separated over a wide area network (WAN).

For more information servers and server properties, see the “Server Properties” appendix in the *SAP BusinessObjects Enterprise Administrator's Guide*.

Service Categories

The Central Management Console (CMC) Server tab groups servers hierarchically by service category. Each service category contains servers that perform similar functions.

The following section describes each service category and the servers it contains.

Core Services

The CMC Servers tab allows you to create new servers by selecting from a list of "Core Services" and choosing a specific service. Depending on the service you select, you may be able to choose other services to be hosted on the server.

Business Process BI Service

Business Process BI Service is a web service that enables BusinessObjects Enterprise technology to be integrated into custom web applications. It receives requests from a web application, coordinates the retrieval and processing of the relevant data, and returns a processed report to the web application.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Central Management Console Service
- Web Services SDK and QaaWS Service

Central Management Console Service

The Central Management Console (CMC) is a web-based administration portal for the Central Management Server (CMS), which, in turn, manages the entire BusinessObjects Enterprise system. The CMC communicates directly with the CMS to view or change configuration settings.

Without the CMC, you cannot manage a BusinessObjects Enterprise deployment.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Business Process BI Service
- Web Services SDK and QaaWS Service

Central Management Service

The Central Management Service receives authentication and report scheduling queries from other BusinessObjects Enterprise servers, and system. This is known as the "CMS system database." All the platform services are managed and controlled by the CMS. The CMS also manages access to the system file store where the physical documents are managed. The system repository database is maintained using the provided database, or by using the supported database of your choice.

Hosted by a Central Management Server. For more information on the Central Management Server, see [Central Management Server](#).

Additional service that can be hosted with this service:

- Single Sign-On Service

Client Auditing Proxy Service

The Client Auditing Proxy Service monitors connected Rich Web Intelligence and Rich Desktop Intelligence clients and forwards the information to the

auditing server. Rich clients working locally, not connected to a repository, are not audited by the Client Auditing Proxy Service.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Publishing Post Processing Service
- Publishing Service
- Search Service

Destination Delivery Scheduling Service

The Destination Delivery Scheduling Service is hosted by a Job Server that runs at a pre-determined time, and publishes the results to the output location specified when the schedule was created. Output can be published to the BusinessObjects Enterprise file system, FTP, SMTP or a user's Inbox.

Hosted by a Job Server. For more information on the Job Server, see [Job Servers](#).

Additional services that can be hosted with this service:

- Destination Configuration Service

Event Service

The Event Service is used to trigger reports to run when a file-based event occurs on a File Repository Server (FRS). For example, if data file is updated or added to an FRS, a report can automatically be run on it.

Hosted by an Event Server. For more information on the Event Server, see [Event Server](#).

No other services run on a server with this service.

Input Filestore Service

The Input Filestore Service maintains a list of published report and program objects that can be used in the generation of new reports. For example, a Job Server requests a report from an Input Filestore service when the report has been scheduled to run. The Input Filestore Service provides the report as 'input' into the reporting process.

Hosted by a File Repository Server. For more information on the File Repository Server, see [File Repository Servers](#) and [Input File Repository Servers](#).

No other services run on this server with this service.

Output Filestore Service

The Output Filestore Service maintains collection of completed reports. For example, a Job Server requests a report from an Output Filestore service when the report has run and the report needs to be sent to a specific destination, such as an user's inbox. The Output Filestore Service provides the report as 'output' of the reporting process.

Hosted by a File Repository Server. For more information on the File Repository Server, see [File Repository Servers](#) and [Output File Repository Servers](#).

No other services run on this server with this service.

Program Scheduling Service

The Program Scheduling Service runs executable objects at a pre-determined time.

Hosted by a Job Server. For more information on the Job Server, see [Job Servers](#).

Additional services that can be hosted with this service:

- Destination Configuration Service

Publishing Post Processing Service

The Publishing Post Processing Service can perform actions on reports after they have completed running. For example, reports can be sent to a variety of destinations, such as a directory or user inbox, upon completion.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Client Auditing Proxy Service
- Publishing Service
- Search Service

Publishing Service

The Publishing Service is the central report publishing service, and coordinates with the Publishing Post Processing Service and Destination Job Service to publish reports the desired destination.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Client Auditing Proxy Service
- Publishing Service
- Search Service

Replication Service

The Replication Service processes replication jobs that mirror reports in different parts of the BusinessObjects Enterprise system.

Hosted by a Job Server. For more information on the Job Server, see [Job Servers](#).

Additional services that can be hosted with this service:

- Destination Configuration Service
- Web Intelligence Scheduling and Publishing Service

Search Service

The Search Service indexes all content in the Central Management Server (CMS) repository. This index is then used when a user searches for a term in BusinessObjects Enterprise clients.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Client Auditing Proxy Service
- Publishing Post Processing Service
- Publishing Service

Web Services SDK and QaaWS Service

The Web Services SDK and Query as a Web Service (QaaWS) service act as a bridge between custom web applications and the BusinessObjects

Enterprise system, allowing developers to implement Business Objects functionality in a custom web application.

Hosted by an Adaptive Processing Server. For more information on the Adaptive Processing Server, see [Adaptive Processing Server](#).

Additional services that can be hosted with this service:

- Business Process BI Service
- Central Management Console Service

Crystal Reports Services

The CMC Servers tab allows you to create new Crystal Reports servers by selecting from a list of "Crystal Reports Services" and choosing a specific service. Depending on the service you select, you may be able to choose other services to be hosted on the server.

Crystal Reports Cache Service

The Crystal Reports Cache Service limits the number of database accesses generated by Crystal Reports by managing a cache of reports. Administrators can configure how long reports are held in the cache, the size of the cache, as well as other properties.

If the Crystal Reports Cache Service is disabled, reports cannot query their data sources.

Hosted by a Crystal Reports Cache Server. For more information on the Crystal Reports Cache Server, see [Crystal Reports Cache Server](#).

No other services run on this server with this service.

Crystal Reports Processing Service

The Crystal Reports Processing Service accepts and processes Crystal Reports. It can share data between reports to reduce the number of database accesses, and can be configured to limit the number of concurrent jobs to prevent the service from becoming overloaded.

Without this service, Crystal Reports cannot be run.

Hosted by a Crystal Reports Processing Server. For more information on the Crystal Reports Processing Server, see [Crystal Reports Processing Server](#).

Additional service that can be hosted with this service:

- Single Sign-On Service

Crystal Reports Scheduling Service

The Crystal Reports Scheduling Service is hosted by a Job Server that runs Crystal Reports at a pre-determined time, then publishes the results to the output location specified when the schedule was created. Reports can be published to the BusinessObjects Enterprise file system, FTP, SMTP or a user's Inbox.

Without this service, you will not be able to schedule Crystal Reports to run unattended, and all Crystal Reports would have to be run manually from the Crystal Reports client.

Hosted by a Job Server. For more information on the Job Server, see [Job Servers](#).

Additional services that can be hosted with this service:

- Destination Configuration Service

Crystal Reports Viewing and Modification Service

Hosted by a Report Application Server. For more information on the Report Application Server, see [Report Application Server](#).

Additional service that can be hosted with this service:

- Single Sign-On Service

List Of Values Scheduling Service

The List of Values Scheduling Service periodically generates a list of options to include in pick-lists. A list of values is a list that contains the distinct data values associated with an object. When you create a dimension or detail object in Universe Designer, it is automatically assigned an associated List Of Values (LOV). This list does not physically exist when you create an object, but by default the object has the ability to query the database to return a list of its values when used to build a query.

Hosted by a Job Server. For more information on the Job Server, see [Job Servers](#).

Additional services that can be hosted with this service:

- Destination Configuration Service

Desktop Intelligence Services

The CMC Servers tab allows you to create new Desktop Intelligence servers by selecting from a list of "Desktop Intelligence Services" and choosing a specific service. Depending on the service you select, you may be able to choose other services to be hosted on the server.

Connection Service

The Connection Service opens and maintains a database or Online Analytical Processing (OLAP) data source connection, through a business view or universe. This allows the Connection Service to act as an intermediary between BusinessObjects Enterprise services and a range of supported data formats.

The Connection Server can also be traced so that database activity can be analyzed and later optimized.

Without the Connection Service running, BusinessObjects Enterprise components will not be able to access a data source.

Hosted by a CS Container Server. For more information on the CS Container Server, see [Connection Server](#).

No other services run on a server with this service.

Desktop Intelligence Cache Service

The Desktop Intelligence Cache Service limits the number of database accesses generated by Desktop Intelligence reports by managing a cache of reports. Administrators can configure how long reports are held in the cache, the size of the cache, as well as other properties.

If the Desktop Intelligence Cache Service is disabled, reports cannot query their data sources.

Hosted by a Desktop Intelligence Cache Server. For more information on the Desktop Intelligence Cache Server, see [Desktop Intelligence Cache Server](#).

No other services run on this server with this service.

Desktop Intelligence Processing Service

The Desktop Intelligence Processing Service accepts and processes Desktop Intelligence reports. It can share data between reports to reduce the number of database accesses, and can be configured to limit the number of concurrent jobs to prevent the service from becoming overloaded.

Without this service, Desktop Intelligence reports cannot be run.

Hosted by a dpsprocFullClient Server.

Additional service that can be hosted with this service:

- Single Sign-On Service

Desktop Intelligence Scheduling Service

The Desktop Intelligence Scheduling Service is hosted by a Job Server that runs Desktop Intelligence reports at a pre-determined time, and publishes the results to the output location specified when the schedule was created. Reports can be published to the BusinessObjects Enterprise file system, FTP, SMTP or a user's Inbox.

Without this service, you will not be able to schedule Desktop Intelligence reports to run unattended, and all Desktop Intelligence reports would have to be run manually from the Desktop Intelligence client.

Hosted by a Job Server. For more information on the Job Server, see [Job Servers](#).

Additional services that can be hosted with this service:

- Destination Configuration Service

Performance Management Services

Services in "Performance Management" services category provide BusinessObjects Enterprise Dashboard and Analytics functionality for data analysis. The following services are used by Dashboard and Analytics:

Service	Hosted by
Dashboard Analytics Service	portfolioEngine Server
Dashboard Service	dashboardEngine Server
PM Metric Aggregation Service	probeEngine Server
PM Repository Management Service	PM Repository Server
PM Rules Service	probeEngine Server
Predictive Analytic Service	Mining Engine Server
Process Analysis Service	spcEngine Server
Sets Profile Service	iProfiler Server
Sets Query Service	queryManager Server

Voyager Services

The CMC Servers tab allows you to create new Multi-Dimensional Analysis server by selecting from a list of "Voyager Services" and choosing a specific service.

Multi-Dimensional Analysis Service

The Multi-Dimensional Analysis Service is hosted by the Multi-Dimensional Analysis Services Server (MDAS) and is used by the Voyager client to access three-dimensional Online Analytical Processing (OLAP) data.

It also converts the raw data into XML packages, which the requesting client application can render into a variety of formats: Excel spreadsheets, PDF, or Voyager crosstabs and charts.

Note:

OLAP single sign-on (SSO) is only supported for Microsoft Analysis Services and SAP BW.

The Multi-Dimensional Analysis Service communicates with the Input File Repository Server (FRS), to retrieve workspaces, and gets data from the OLAP database server. As the Voyager client renders results on the web application server, the Multi-Dimensional Analysis Service returns results to

the client in XML format, which is formatted and displayed by the Voyager client.

There are no additions services hosted with this service.

For more information, see [Multi-Dimensional Analysis Services \(MDAS\) Server](#). To read an example workflow of the Multi-Dimensional Analysis Services Server viewing a workspace, see [Viewing a Voyager workspace](#).

Web Intelligence Services

The CMC Servers tab allows you to create new Web Intelligence servers by selecting from a list of "Web Intelligence Services" and choosing a specific service. Depending on the service you select, you may be able to choose other services to be hosted on the server.

Web Intelligence Processing Service

The Web Intelligence Processing Service is a subsystem of the Web Intelligence Processing Server that runs Web Intelligence reports submitted to the server by Web Intelligence clients and the Web Intelligence Scheduling and Publishing Service. The resulting Web Intelligence report is the passed back to the originator.

Although the Web Intelligence Processing Service does not query the database or generate the final report itself, it does coordinate with Input and Output File Servers (to fetch the document on which the report is based) and the Report Engine and Connection Servers (to retrieve data from the Universe, or database, and process the report).

Without at least one Web Intelligence Processing service running, Web Intelligence clients would not be able to open, view, or run reports, and scheduled Web Intelligence reports would fail to run.

For more information on the Web Intelligence Processing Server, see [Web Intelligence Processing Server](#). For information about scheduled Web Intelligence reports, see [Web Intelligence Scheduling and Publishing Service](#). For Web Intelligence workflow scenarios, see the [Scheduling](#) and [Viewing](#) sections of [Information Workflows](#).

Additional service that can be hosted with this service:

- Single Sign-On Service

Web Intelligence Scheduling and Publishing Service

The Web Intelligence Scheduling and Publishing Service is hosted by an Adaptive Job Server that runs Web Intelligence reports at a pre-determined time, and publishes the results to the output location specified when the schedule was created. You can schedule Web Intelligence reports with the Central Management Console (CMC). Reports can be published to the BusinessObjects Enterprise file system, FTP, SMTP or a user's Inbox.

Without this service, you will not be able to schedule Web Intelligence reports to run unattended, and all Web Intelligence reports would have to be run manually from the Web Intelligence client.

The Web Intelligence Scheduling and Publishing Service is hosted by an Adaptive Job Server. For more information on Adaptive Job Servers, see [Adaptive Job Server](#).

Additional services that can be hosted with this service:

- Destination Configuration Service (allows reports to be sent to different locations).
- Replication Service

Xcelsius Services

The CMC Servers tab allows you to create new Xcelsius servers by selecting from a list of "Xcelsius Services" and choosing a specific service. Depending on the service you select, you may be able to choose other services to be hosted on the server.

Xcelsius Cache Service

The Xcelsius Cache Service limits the number of database access requests generated by Xcelsius by managing a cache of query results. Administrators can configure how long data is held in the cache, the size of the cache, as well as other properties.

If the Xcelsius Cache Service is disabled, dashboards cannot query their data sources.

Hosted by a Xcelsius Cache Server.

No other services run on this server with this service.

Xcelsius Processing Service

The Xcelsius Processing Service accepts and processes Xcelsius queries. It can share data between queries to reduce the number of database accesses, and can be configured to limit the number of concurrent jobs to prevent the service from becoming overloaded.

Hosted by a Xcelsius Processing Server.

Additional service that can be hosted with this service:

- Single Sign-On Service

Adaptive Job Server

The Adaptive Job Server is a specialized job server that hosts BusinessObjects Enterprise services, such as the Replication Service, Web Intelligence Scheduling and Publishing Services, and the Destination Configuration Service.

The Adaptive Job Server runs as a container for the selected services, which all run under a single account in the same memory space and under the same process id (PID). If you stop the Adaptive Job Server, you stop all of the contained job services.

An Adaptive Job Server can host the following services:

- Destination Configuration Service
- Web Intelligence Scheduling and Publishing Service (runs and publishes Web Intelligence reports at a pre-determined time).
- Replication Service

See also: [Job Servers](#).

Example:

The following Adaptive Job Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.AdaptiveJobServer`

Adaptive Processing Server

An Adaptive Processing Server is a generic server that hosts services responsible for processing requests from a variety of sources. An Adaptive Processing Server can host the following services:

- Business Process BI Service
- Client Auditing Proxy Service (collects auditing information from connected Rich Desktop and Web Intelligence Clients).
- Publishing Post Processing Service (responsible for any post processing of a publication job, including PDF merging and publication extension processing).
- Publishing Service (coordinates the publication of an object by communicating with other services).
- Search Service (processes search requests and executes the indexing).

Example:

The following Adaptive Processing Servers are created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.AdaptiveProcessingServer
-

Central Management Server

The Central Management Server (CMS) maintains a database of information about your BusinessObjects Enterprise system. This is known as the "CMS system database." All the platform services are managed and controlled by the CMS. The CMS also manages access to the system file store where the physical documents are managed. The system repository database is maintained using the provided database, or by using the supported database of your choice.

CMS data includes information about users and groups, security levels, content, and services. The CMS can also maintain an optional auditing database of information about user actions, to perform four main tasks:

- Maintaining security

The CMS enforces the application of rights at both the folder and object level, and supports inheritance at the user and group level. It also supports aggregation through a flexible, group-user membership model.

An integrated security system is available for customers who do not currently use an entitlement database, although BusinessObjects Enterprise is designed for integration with multiple concurrent third-party security systems, such as LDAP, Siteminder, or Microsoft Active Directory. When a change is made to a user in the entitlement database, the change is then propagated to BusinessObjects Enterprise.

- Managing objects

The CMS keeps track of the object location and maintains the folder hierarchy. “InfoObjects” are system metadata objects that contain index information, and the actual documents or objects are stored in a file store. The separation of the object definition (metadata) from the document allows for fast object processing as only the required information is retrieved from the system's repository. The CMS also runs scheduled report jobs.

- Managing servers

The CMS handles load balancing and automated clustering to avoid bottlenecks and maximize hardware efficiency. In some multi-server environments, BusinessObjects Enterprise may not require a separate third-party load balancing system.

- Managing auditing

User actions can be monitored and written to a central audit database. This information allows system administrators to better track and manage their BusinessObjects Enterprise deployment.

The auditing functionality allows administrators to better understand which users accessed the enterprise system, which documents they interacted with. Usage data is collected from the system interactions recorded in the auditing database. A sample universe and sample auditing reports are also available to provide fast access to information such as the most accessed reports, peak system use times, and average user session times.

Note:

It is strongly recommended that you back up and audit the CMS system database frequently.

Caution:

The CMS database should not be accessed directly. System information should only be retrieved using the calls that are provided in the BusinessObjects Enterprise software development kit (SDK).

Restriction:

You may access the optional audit database in read-only mode to create custom audit reports.

On Windows, the Setup program can install and configure its own database if you do not already have a database server allocated for the deployment. You can switch to a different database later if your deployment needs change.

A Central Management Server hosts the following services:

- Central Management Service (core CMS service).
- Single Sign-On Service (allows users to sign on to BusinessObjects Enterprise with credentials from a common authentication system).

Example:

The following Central Management Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.CentralManagementServer`
-

Connection Server

Responsible for handling connection and interaction with the various datasources and providing a common feature set to its clients, by emulating the missing features if necessary.

The Connection Server provides database access to the raw source data. It supports relational databases (Oracle, MySQL, Microsoft SQL Server, DB2, Sybase) as well as OLAP (SAP BW, Microsoft Analysis Services, Hyperion Essbase). The Connection Server is responsible for handling connection and interaction with the various datasources and providing a common feature set to its clients, by emulating the missing features if necessary.

The Connection Server can be accessed through a Dynamic Link Library (inproc), a CORBA server (called through CORBA or HTTP), or by using the Java API.

A Connection Server hosts the following service:

- Connection Service (provides a database connection to other servers).

Example:

The following Connection Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.ConnectionServer
-

Crystal Reports Cache Server

The Crystal Reports Cache Server intercepts report requests sent from clients to the page server. If the cache server cannot fulfill the request with a cached report page, it passes the request on to the page server, which runs the report and returns the results. The cache server then caches the report page for future use, and sends the report to the viewer.

A Crystal Reports Cache Server hosts the following service:

- Crystal Reports Cache Service (creates and maintains a cache of recently-viewed reports).

Example:

The following Crystal Reports Cache Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.CrystalReportsCacheServer
-

Crystal Reports Processing Server

The Crystal Reports Processing Server is responsible for responding to page requests by processing reports and generating encapsulated page format (EPF) pages. The key benefit of EPF is that it supports page-on-demand access so only the requested page is returned, instead of the entire report.

This enhances performance and reduces unnecessary network traffic for large reports.

The EPF pages contain formatting information that defines report layout. The Processing Server retrieves data for the report from an instance or directly from the database (depending on the user request and the rights he or she has to the report object). When retrieving data from the database, the Processing Server automatically disconnects from the database after it fulfills its initial request and if necessary, reconnects to retrieve additional data. This helps conserve database traffic and limit the unnecessary use of database licenses.

The Cache Server and Processing Server work closely together. Specifically, the Processing Server responds to page requests made by the Cache Server. The Processing Server and Cache Server also interact to ensure cached EPF pages are reused as frequently as possible, and new pages are generated as required. BusinessObjects Enterprise takes advantage of this behavior by ensuring that the majority of report-viewing requests are made to the Cache Server and Processing Server. However, if a user's default viewer is the DHTML viewer, the report is processed by the Report Application Server.

Runs Crystal report queries and returns data to Crystal Reports Cache Server.

A Crystal Reports Processing Server hosts the following services:

- Crystal Reports Processing Service
- Single Sign-On Service

Example:

The following Crystal Reports Processing Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.CrystalReportsProcessingServer

Dashboard Analytics Server

Server process used by the Dashboard Builder component to create and manage corporate and personal dashboard analytic content.

A Dashboard Analytics Server hosts the following service:

- Dashboard Analytics Service (provides core Dashboard Analytics functionality).

Example:

The following Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.DashboardAnalyticsServer
-

Dashboard Server

Server process used by the Dashboard Builder component to create and manage corporate and personal dashboards. Dashboard Builder offers metrics, alerts, and dashboard management capabilities to help organizations monitor and understand their business activities.

A Dashboard Server hosts the following service:

- Dashboard Service (provides core Dashboard functionality).

Example:

The following Dashboard Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.DashboardServer
-

Desktop Intelligence Cache Server

The Desktop Intelligence Cache Server intercepts report requests sent from clients to the page server. If the cache server cannot fulfill the request with a cached report page, it passes the request on to the page server, which runs the report and returns the results. The cache server then caches the report page for future use, and sends the report to the viewer.

A Desktop Intelligence Cache Server hosts the following service:

- Desktop Intelligence Cache Service (creates and maintains a cache of viewed reports).

Example:

The following Desktop Intelligence Cache Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.DesktopIntelligenceCacheServer`
-

Desktop Intelligence Job Server

The Desktop Intelligence Job Server processes scheduling requests received from the CMS for Desktop Intelligence documents, and generates the instance of the Desktop Intelligence document.

A Desktop Intelligence Job Server hosts the following services:

- Destination Configuration Service
- Desktop Intelligence Scheduling Service

Example:

The following Desktop Intelligence Job Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.DesktopIntelligenceJobServer`

See also: [Job Servers](#).

Desktop Intelligence Processing Server

A Desktop Intelligence Processing Server hosts the following services:

- Desktop Intelligence Processing Service (processes viewing requests for Desktop Intelligence documents, generating Desktop Intelligence documents).
- Single Sign-On Service (allows users to sign on to BusinessObjects Enterprise with credentials from a common authentication system).

Example:

The following Desktop Intelligence Processing Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.DesktopIntelligenceProcessingServer
-

Event Server

The Event Server monitors the system for events, which can act as a trigger for running a report. When you set up a event trigger within BusinessObjects Enterprise, the Event Server monitors the condition and notifies the CMS that the file-based event has occurred. The CMS can then start any jobs that are dependent upon the event occurring.

Note:

Schedule-based and custom events are managed through the CMS.

An Event Server hosts the following service:

- Event Service (monitors file-based events)

Example:

The following Event Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.EventServer
-

File Repository Servers

File repository servers are responsible for the creation of file system objects, such as exported reports, and imported files in non-native formats.

Input and Output File Repository Server (FRS) processes run on each BusinessObjects Enterprise server machine.

The FRSEs are responsible for listing files on the server, querying for the size of a file, querying for the size of the entire file repository, adding files to the repository, and removing files from the repository.

Caution:

To avoid conflicts between input and output objects, the Input and Output FRSes cannot share the same file system directory. In larger deployments, there may be multiple Input and Output FRSes. All Input File Repository Servers share the same directory. Likewise, all Output File Repository Servers share the same directory.

Input File Repository Servers

The Input FRS stores report and program objects that have been published to the system by administrators or end users (using the Publishing Wizard, the CMC, the Import Wizard, or a Business Objects designer component such as Crystal Reports, or Web Intelligence report panels).

Note:

Objects with associated files, such as text files, Microsoft Word files, or PDFs, are stored on the Input File Repository Server.

A Input File Repository Server hosts the following service:

- Input Filestore Service

The following Input File Repository Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.InputFileRepository`

Output File Repository Servers

The Output FRS stores all of the report instances generated by the Report Job Server or the Web Intelligence Processing Server, and the program instances generated by the Program Job Server.

Tip:

If you use the BusinessObjects Enterprise SDK, you can also publish reports from within your own code.

An Output File Repository Server hosts the following service:

- Output Filestore Service

The following Output File Repository Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.OutputFileRepository

Job Servers

A Job Servers is a generic process that processes scheduled actions on objects at the request of the CMS. When you add a Job server to the BusinessObjects Enterprise system, you can configure the Job server to:

- Process report and document objects.
- Process program objects.
- Process publication objects.
- Send objects or instances to specified destinations.

A Job Server can host the following services:

- Destination Configuration Service
- Web Intelligence Scheduling and Publishing Service
- Replication Service

See also: [Adaptive Job Server](#).

Example:

The following Job Servers are created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.AdaptiveJobServer
 - <HOSTNAME>.CrystalReportsJobServer
 - <HOSTNAME>.DesktopIntelligenceJobServer
 - <HOSTNAME>.DestinationJobServer
 - <HOSTNAME>.ListOfValuesJobServer
 - <HOSTNAME>.ProgramJobServer
 - <HOSTNAME>.PublicationJobServer
 - <HOSTNAME>.WebIntelligenceProcessingServer
-

List of Values Job Server

The List of Values Job Server is a specialized container that manages lists of distinct data values associated with an object in the BusinessObjects Enterprise system.

A list of values is a selection of valid terms that can be used in the context of a specific query or phrase. This reduces the likelihood of an invalid query or phrase being created.

Example:

The following List of Values Job Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.ListOfValuesJobServer`

See also: [Job Servers](#).

Multi-Dimensional Analysis Services (MDAS) Server

The Multi-Dimensional Analysis Services (MDAS) Server is a container for the Multi-Dimensional Analysis Service, which provides the BusinessObjects Voyager client with an extensible framework for accessing multi-dimensional Online Analytical Processing (OLAP) data.

To avoid delays in processing OLAP client requests, run multiple MDAS Servers on several different machines. Disabling this server will prevent the Voyager client from accessing OLAP data sources.

For more information on the Multi-Dimensional Analysis Service, see [Multi-Dimensional Analysis Services \(MDAS\) Server](#). To read an example workflow of the Multi-Dimensional Analysis Services Server viewing a workspace, see [Viewing a Voyager workspace](#).

Example:

The following Multi-Dimensional Analysis Services Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.MultiDimensionalAnalysisServicesServer
-

PM Metrics Server

Dashboard and Analytics server to populate metrics created using the Metric Engine. For more information, consult the *Dashboard and Analytics Setup and Administration Guide*.

A PM Metrics Server hosts the following service:

- PM Metric Aggregation Service

Example:

The following PM Metrics Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.PMMetricsServer
-

PM Repository Server

Dashboard and Analytics server to read and store performance information from the Dashboard and Analytics repository.

A PM Repository Server hosts the following service:

- PM Repository Management Service

Example:

The following PM Repository Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.PMRepositoryServer
-

PM Rules Server

Dashboard and Analytics server to create rules and alerts. Rules and alerts automate the process of detecting and interpreting change, and delivering relevant analysis. Rules enable you to proactively monitor your business and take appropriate and timely action in response to specific events. For more information, consult the *Dashboard and Analytics Setup and Administration Guide*.

A PM Rules Server hosts the following service:

- PM Rules Service

Example:

The following PM Rules Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.PMRulesServer
-

Predictive Analysis Server

Server used for Predictive Analysis (Data Mining) using KXEN engine, which quickly uncovers key business drivers from your data and forecasts future business conditions. It helps users make proactive decisions more easily by providing insight in familiar terms through dashboards across the organization. For more information, consult the *Dashboard and Analytics Setup and Administration Guide*.

A Predictive Analysis Server hosts the following service:

- Predictive Analytic Service

Example:

The following Predictive Analysis Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.PredictiveAnalysisServer
-

Process Analysis Server

The process analysis server monitors server activity. This helps your organization to automate the tracking of quality variables by using alarm rules and control chart types defined by your quality improvement initiatives. For more information, consult the *Dashboard and Analytics Setup and Administration* Guide.

A Process Analysis Server hosts the following service:

- Process Analysis Service

Example:

The following Process Analysis Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.ProcessAnalysisServer
-

Program Job Server

A Program Job Server runs executable objects at a pre-determined time.

A Job Server hosts the following services:

- Destination Configuration Service
- Web Intelligence Scheduling and Publishing Service
- Replication Service

Example:

The following Program Job Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.ProgramJobServer

See also: [Job Servers](#).

Publication Job Server

The Publication Job Server processes requests that it receives from the CMC or InfoView and sends the requested objects or instances to the specified destination. If the request is for an object, the Publication Job Server retrieves the object from the Input File Repository Server. If the request is for a report or program instance, the Publication Job Server retrieves the instance from the Output File Repository Server. The Publication Job Server can send objects and instances to a destination inside the BusinessObjects Enterprise system, such as a user's inbox. It can also send objects outside the system, via e-mail.

A Publication Job Server hosts the following services:

- Destination Configuration Service
- Web Intelligence Scheduling and Publishing Service
- Replication Service

Example:

The following Publication Job Server is created by the BusinessObjects Enterprise setup program:

- `<HOSTNAME>.PublicationJobServer`

See also: [Job Servers](#).

Report Application Server

Provides ad-hoc reporting capabilities that allow users to create and modify Crystal reports via the RAS Software Development Kit (SDK). This SDK supports the Java viewer SDKs and does not require a specific license; it is included with your BOE package.

The RAS is also used to resolve Dynamic Recipient Lists at runtime or during the design phase when working with publications, as well as with LiveOffice.

Example:

The following Report Application Server is not created by the BusinessObjects Enterprise setup program by default:

- <HOSTNAME>.ReportApplicationServer
-

Sets Profile Server

Manages Performance Management profile information.

A Sets Profile Server hosts the following service:

- Sets Profile Service

Example:

The following Sets Profile Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.SetsProfileServer
-

Sets Query Server

Runs Performance Management set queries.

A Sets Query Server hosts the following service:

- Sets Query Service

Example:

The following Sets Query Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.SetsQueryServer
-

Web Intelligence Processing Server

A Web Intelligence Processing Server is a specialized Job Server that accepts a Web Intelligence report, coordinates with other servers to run the report, and returns the result to the originator.

Each Web Intelligence Processing Server can be configured with a maximum number of concurrent jobs (Maximum Jobs Allowed) value. To ensure that server performance is not degraded by a large number of concurrent jobs, run multiple Web Intelligence Processing Servers on different machines.

A Web Intelligence Processing Server hosts the following services:

- Single Sign-On Service
- Web Intelligence Processing Service

For more information, see [Web Intelligence Processing Service](#).

Example:

The following Web Intelligence Processing server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.WebIntelligenceProcessingServer
-

Web Application Container Server (WACS)

The Web Application Container Server allows the Central Management Console (CMC) to run on installations that do not include a Java web application server, or those that want to maintain separation between the CMC and web applications on the deployment web application server.

A Web Application Container Server hosts the following service:

- Web Application Container Service.
- Central Management Console Service.

Example:

The following Web Application Container Server is created by the BusinessObjects Enterprise setup program, if you opted to install it:

- <HOSTNAME>.WebApplicationContainerServer
-

Xcelsius Cache Server

The Xcelsius Cache Server intercepts query requests sent from clients to the page server. If the cache server cannot fulfill the request with a cached dashboard object, it passes the request on to the page server, which runs the query and returns the results. The cache server then caches the dashboard object for future use, and sends the object to the viewer.

A Xcelsius Cache Server hosts the following service:

- Xcelsius Cache Service (creates and maintains a cache of recently-viewed dashboards).

Example:

The following Xcelsius Cache Server can be created by the Central Management Console:

- <HOSTNAME>.XcelsiusCacheServer
-

Crystal Reports Processing Server

The Crystal Reports Processing Server is responsible for responding to page requests by processing reports and generating encapsulated page format (EPF) pages. The key benefit of EPF is that it supports page-on-demand access so only the requested page is returned, instead of the entire report. This enhances performance and reduces unnecessary network traffic for large reports.

The EPF pages contain formatting information that defines report layout. The Processing Server retrieves data for the report from an instance or directly from the database (depending on the user request and the rights he or she has to the report object). When retrieving data from the database, the Processing Server automatically disconnects from the database after it fulfills its initial request and if necessary, reconnects to retrieve additional data. This helps conserve database traffic and limit the unnecessary use of database licenses.

The Cache Server and Processing Server work closely together. Specifically, the Processing Server responds to page requests made by the Cache Server. The Processing Server and Cache Server also interact to ensure cached EPF pages are reused as frequently as possible, and new pages are generated as required. BusinessObjects Enterprise takes advantage of this behavior by ensuring that the majority of report-viewing requests are made to the Cache Server and Processing Server. However, if a user's default viewer is the DHTML viewer, the report is processed by the Report Application Server.

Runs Crystal report queries and returns data to Crystal Reports Cache Server.

A Crystal Reports Processing Server hosts the following services:

- Crystal Reports Processing Service
- Single Sign-On Service

Example:

The following Crystal Reports Processing Server is created by the BusinessObjects Enterprise setup program:

- <HOSTNAME>.CrystalReportsProcessingServer
-

Web application servers

A third-party web application server acts as the translation layer between the end user's web browser and BusinessObjects Enterprise Software Development Kit (SDK) interface running on a web application server. Web application servers running on Windows, Unix, and Linux are supported.

You can use a combination of these options:

1. A Java web application server (Windows, Unix, Linux)

The setup program can also automatically deploy InfoView and the CMC to:

- Tomcat 5.5
- WebLogic 9
- WebLogic 10
- WebSphere 6.1
- Oracle Application Server 10g R3

- Sun Java Application Server 9.0

The following web application servers are also supported, but InfoView and the CMC must be manually deployed:

- SAP web application server 7
- WebSphere Community Edition 2.0
- Jboss 4.04

Note:

The BusinessObjects Enterprise setup program will install and deploy InfoView and the CMC to Tomcat 5.5 by default.

2. Microsoft Internet Information Server (IIS) .NET web application server (Windows only)

InfoView is supported on Microsoft Information Server (IIS), and, when detected, the BusinessObjects Enterprise setup program will automatically install and deploy InfoView to IIS.

The CMC is not supported on IIS. In order to manage your BusinessObjects Enterprise system with the CMC, you must deploy the CMC to a Java web application server or install the Web Application Container Service (WACS).

3. Web Application Container Service (WACS)

If you plan to use .NET InfoView, and you do not want to use a Java application server to host your CMC, then you can use WACS to host the Central Management Console (CMC).

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

Web applications such as the CMC are automatically deployed to WACS. WACS does not support deploying Business Objects or external web applications, whether manually or by using wdeploy.

Java SDK

The BusinessObjects Enterprise Java 2 Enterprise Edition (J2EE) software development kit (SDK) allows you to create Java web applications that run on the web application server in your BusinessObjects Enterprise deployment.

SDKs give you the ability to create web applications that integrate powerful reporting features, such as those offered by Web Intelligence or InfoView.

The following Java SDKs are included with BusinessObjects Enterprise.

- BusinessObjects Enterprise Java SDK.
- Report Engine Java SDK.
- Report Application Server (RAS) Java SDK.
- Viewers Java SDK.
- Web services Java SDK.
- JavaServer Faces Components (JSF) for BusinessObjects Enterprise SDK.

BusinessObjects Enterprise Java SDK

The BusinessObjects Enterprise Java SDK allows you to incorporate BusinessObjects Enterprise functionality into your own web applications.

1. Authentication and session management.

Users can be authenticated by using the BusinessObjects Enterprise authentication protocol or some other protocol, such as LDAP or Kerberos. Once the user is authenticated, a user session is created. The user session maintains state information as the user performs actions and navigates to different pages within the BusinessObjects Enterprise web application.

2. Working with repository objects.

The information entity in BusinessObjects Enterprise is the InfoObject. All operations involve the retrieval and manipulation of InfoObjects from the Central Management Server (CMS).

3. Report operations.

The BusinessObjects Enterprise Java SDK supports many types of report documents: Crystal reports, Web Intelligence and Desktop Intelligence documents, as well as Microsoft Excel, and Adobe's Portable Document Format (PDF), among others.

4. Administering BusinessObjects Enterprise.

Many aspects of a BusinessObjects Enterprise deployment can be administered programmatically, such as managing server process and server process groups, and server auditing.

Report Engine Java SDK

The Report Engine Java SDK includes libraries that you can use to build a web report design tool. Applications built with this SDK can view, create, or modify, a variety of different Web Intelligence and Desktop Intelligence documents. Users can modify documents by adding, removing, and modifying objects such as tables, charts, conditions, and filters.

Report Application Server (RAS) Java SDK

The Report Application Server (RAS) Java SDK is an API for developing Java web applications with advanced report creation and modification functionality. With the RAS Java SDK, you can create Java client applications that interact with the RAS server from a web application server.

Web application users can create or modify Crystal reports by adding, removing, or modifying tables, charts, parameters, and fields.

Viewers Java SDK

The Viewers SDK is an API that lets you incorporate reports in a range of different formats within your web application.

Viewers are a 'thin-client' technology - users of your web application don't need to install any additional software in order to view the reports. Two Java viewers are available:

1. DHTML report page viewer.

This viewer provides basic thin-client report viewing capabilities to present data and allow drill-down, page navigation, zooming, prompting, text searching, highlighting, exporting, and printing.

2. Report parts viewer.

This viewer provides the ability to view individual report parts including charts, text, and fields.

JavaServer Faces (JSF) SDK

The JavaServer Faces (JSF) SDK consists of JavaServer Faces components and managed Java beans built on top of the BusinessObjects EnterpriseJava SDK. The components encapsulate common BusinessObjects Enterprise functionality, such as logging on to the system, navigating through folders and categories, listing managed content, and viewing Crystal reports.

JSF component functionality can be divided into several main areas of BusinessObjects Enterprise application development.

1. Identifying end users in a BusinessObjects Enterprise system.

Individual users can be associated with their actions, such as logging on or off, and changing a password.

2. Listing and navigating managed content.

Users can navigate repetitive information using nested lists rendered from a data source.

3. Scheduling of managed content.

Your application's users can schedule reports to run at custom intervals if you create pages that enable a user to set scheduling options.

4. Viewing managed content.

The `ReportPageViewer` component lets you quickly add the ability to view reports on a page.

.NET SDK

The BusinessObjects Enterprise .NET software development kit (SDK) allows you to create .NET web applications that run on the web application server in your BusinessObjects Enterprise deployment.

SDKs give you the ability to create web applications that integrate powerful reporting features, such as those offered by Crystal Reports or InfoView.

Web applications that use the SDK run within the web application server and connect to the Report Application Server (RAS) running in the BusinessObjects Enterprise processing tier.

BusinessObjects Enterprise installations that use the .NET Framework include Primary Interop Assemblies (PIAs) that allow you to use the BusinessObjects Enterprise .NET SDK with ASP.NET, and a set of .NET Server Components that you can use to simplify the development of custom applications. This configuration requires the use of a Microsoft Internet Information Services (IIS) web server.

The following .NET SDKs are included with BusinessObjects Enterprise.

- BusinessObjects Enterprise .NET SDK.
- Report Engine .NET SDK
- Report Application Server (RAS) .NET SDK.
- Crystal Reports .NET SDK.
- Web services .NET SDK.

BusinessObjects Enterprise .NET SDK

The BusinessObjects Enterprise .NET SDK allows you to incorporate BusinessObjects Enterprise functionality into your own web applications.

1. Authentication and session management.

Users can be authenticated by using the BusinessObjects Enterprise authentication protocol or some other protocol, such as LDAP or Kerberos. Once the user is authenticated, a user session is created. The user session maintains state information as the user performs actions and navigates to different pages within the BusinessObjects Enterprise web application.

2. Working with repository objects.

The information entity in BusinessObjects Enterprise is the InfoObject. All operations involve the retrieval and manipulation of InfoObjects from the Central Management Server (CMS).

3. Report operations.

The BusinessObjects Enterprise .NET SDK supports many types of report documents: Crystal reports, Web Intelligence and Desktop Intelligence documents, as well as Microsoft Excel, and Adobe's Portable Document Format (PDF), among others.

4. Administering BusinessObjects Enterprise.

Many aspects of a BusinessObjects Enterprise deployment can be administered programmatically, such as managing server process and server process groups, and server auditing.

Report Engine .NET SDK

The Report Engine .NET SDK includes libraries that you can use to build a web report design tool. Applications built with this SDK can view, create, or modify, a variety of different Web Intelligence and Desktop Intelligence documents. Users can modify documents by adding, removing, and modifying objects such as tables, charts, conditions, and filters.

Report Application Server (RAS) .NET SDK

The Report Application Server (RAS) SDK is a API for developing .NET web applications with advanced report creation and modification functionality. With the RAS .NET SDK, you can create .NET client applications that interact with the RAS server from a web application server.

Web application users can create or modify Crystal reports by adding, removing, or modifying tables, charts, parameters, and fields.

Crystal Reports .NET SDK

The Crystal Reports .NET SDK allows you to incorporate BusinessObjects Enterprise functionality into your own web applications, including:

1. Core functions.
 Embed Crystal Reports Designer in your applications for report creation.
2. Database connections.
 Log on to a database server and access data.
3. Report data manipulation.
 Filter, group, sort, and total report data.
4. Report appearance and report objects.
 Format, work with field and text objects, and enhance report presentation.
5. Printing and Exporting.
 Export reports to other formats, and print reports.

Web Services

Business Objects Web Services provide a Java API accessed by rich clients in the user interaction tier, such as Live Office and Crystal Reports.

Web Services consists of software components that can be called remotely using the Simple Object Access Protocol (SOAP). SOAP is a protocol for exchanging information that is not dependent on a specific platform, object model, or programming language.

BusinessObjects Enterprise Web Services includes functionality in the following areas:

- Session
 Authentication and user privilege management.
- BI platform
 Exposes advanced platform features such as scheduling, search, user and group administration, server administration, platform events, and calendars.
- Report Engine
 Displays Web Intelligence and Crystal Reports in HTML, PDF, Excel, and XML format.

- Query

Builds ad-hoc queries based on the Business Objects universe semantic layer.

Business Objects web services uses standards such as XML, SOAP, AXIS 2.0 and WSDL. The platform follows *WS-Interoperability Basic Profile 1.0* web services specification.

Note:

Web Services applications are currently only supported with the following load balancer configurations:

1. Source IP address persistence.
2. Source IP and destination port persistence (available only on a Cisco Content Services Switch).
3. SSL persistence.

Note:

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

For information on installing and configuring Web Services, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Query as a Web Service

Business Objects Query as a Web Service is a wizard-based application that allows queries to be made into a web service and integrated with web-ready applications. Queries can be saved to create a catalog of standard queries that application builders can select as required.

Business Intelligence (BI) content is usually bound to a specific user interface of BI tools. Query as a Web Service changes this by allowing BI content to be delivered to any user interface that can process web services.

Query as a Web Service is designed to work on top of any Microsoft Windows application the same way as other web services. Query as a Web Service is based on the W3C web service specifications SOAP, WSDL, and XML. It has two main components:

1. Server component

The server component (included in BusinessObjects Enterprise) stores the Query as a Web Service catalog and hosts the published web services.

2. Client tool

This is how business users create and publish their queries as a web service on the server. You can install the client tool on several machines that can access and share the same Query as a Web Service catalog stored on the server. The client tool communicates with the server components via web services.

Query as a Web Service allows web queries to be used as part of a range of client-side solutions.

- Microsoft Office, Excel, and InfoPath.
- SAP Application Server.
- OpenOffice.
- Business rules and process management applications.
- Enterprise Service Bus platforms.

Web Application Container Service (WACS)

If you plan to use .NET InfoView, and you do not want to use a Java application server to host your CMC, then you can use WACS to host the Central Management Console (CMC).

If you plan to use a supported Java application server to deploy BusinessObjects Enterprise web applications, or if you are installing BusinessObjects Enterprise on a UNIX system, you do not need to install and use WACS.

Using WACS to host the CMC provides you with a number of advantages:

- WACS requires a minimum effort to install, maintain, and configure.
- All hosted applications are predeployed on WACS, so that no additional manual steps are required.
- WACS is supported by Business Objects.
- WACS removes the need for Java application server administration and maintenance skills.
- WACS provides an administrative interface that is consistent with other Business Objects servers.

Databases

BusinessObjects Enterprise uses three different of databases:

1. System database

An internal database that stores configuration, authentication, user, and other information related to BusinessObjects Enterprise. System databases can be created and used on a wide variety of database platforms.

2. Reporting database

Your organization's database, used to create reports, generate statistics, and collect business intelligence. An even wider variety of database platforms are supported for reporting databases than for system databases.

3. Auditing database

An internal database that stores information on security events such as user login, logout, and object access events.

Please review the online BusinessObjects Enterprise supported platforms document for information related to supported database release versions, patch levels, or caveats at the Business Objects customer support site: http://support.businessobjects.com/documentation/supported_platforms.

System databases

Central Management System (CMS) Database

The Central Management System (CMS) server is the only server that accesses the CMS system database. The CMS can also maintain an optional auditing database of information about user actions with the Enterprise system. The data stored inside the CMS system database allows the CMS to perform the following tasks:

- Maintaining security

The CMS enforces the application of all rights at the global, folder, and object level, and supports inheritance at the user and group level.

- Managing objects

The CMS keeps track of the object location and maintains the folder hierarchy. InfoObjects are system metadata objects that contain index information. The actual documents/objects are stored in the FRS. The separation of the object definition (metadata) from the actual document allows the system to retrieve only the required information from the system database, thus providing faster object processing.

- Managing servers

The CMS handles load balancing to help avoid bottlenecks and maximizes hardware efficiency.

You provide the CMS with database connectivity and credentials when you install BusinessObjects Enterprise, so the CMS can create the CMS database using your organization's preferred database servers. Before you install and connect the CMS to your own database server, you must create a new, empty database on your database server.

Note:

- It is strongly recommended that you backup the CMS database and audit the database frequently.
- The CMS database cannot be accessed or modified directly. You should only make changes to the system database through BusinessObjects Enterprise interfaces such as the CMC that interact with the CMS.
- Administrators can access the audit database directly to create custom audit reports.

Reporting databases

Universes

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

Universes are a core component of BusinessObjects Enterprise. All universe objects and connections are stored and secured in the central repository by the Connection Server. Universe designers need to login to BusinessObjects Enterprise to access the system and create universes. Universe access and row-level security can also be managed at the group or individual user level from within the design environment.

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

Views

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

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

BusinessObjects Enterprise includes a series of dedicated, pre-configured platform management services for tasks such as password management, server metrics, and user access control for decentralized management functions.

Auditing database

The CMS acts as the system auditor; the BusinessObjects Enterprise server that you monitor is the auditee.

As the auditor, the CMS controls the overall audit process. Each server writes audit records to a log file local to the server. At regular intervals, the CMS communicates with the auditee servers to request copies of records from the auditee's local log files. When the CMS receives these records it writes data from the log files to the central auditing database.

The CMS also controls the synchronization of audit actions that occur on different machines. Each auditee provides a time stamp for the audit actions that it records in its log file. To ensure that the time stamps of actions 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, the auditees correct the time stamps that are recorded in their log files for subsequent audit actions.

Note:

- You must configure the auditing database on the CMS before you can begin to audit.
- The CMS acts as both an auditor and as an auditee when you configure it to audit an action that the CMS controls.
- In a CMS cluster, the cluster assigns the first CMS to start to act as a system auditor. If the machine that is running this CMS fails, another CMS from the cluster takes over and begins acting as the auditor.

Authentication and single sign-on

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

This section discusses key components of system security, including:

- CMS security.
- Third-party security plug-ins.

Note:

Because these components are responsible for additional tasks, several are described in more detail in other sections.

Central Management Server (CMS) security

The CMS handles security information, such as user accounts, group memberships, and object rights that define user and group privileges.

When you set up your system, the CMS allows you to create user accounts and groups within BusinessObjects Enterprise, or reuse existing user accounts and groups that are stored in a third-party system (such as LDAP or Windows Active Directory). The CMS supports third-party authentication, so users can log into BusinessObjects Enterprise with their current LDAP, or Windows AD credentials.

When users log on, the CMS coordinates the authentication process with its security plug-ins; the CMS then grants the user a logon token and an active session on the system. The CMS also responds to authorization requests made by the rest of the system. When a user requests a list of reports in a particular folder, the CMS authorizes the request only when it has verified that the user's account or group membership has sufficient privileges.

Security plug-ins

Security plug-ins expand and customize the ways in which users are authenticated. BusinessObjects Enterprise ships with the BusinessObjects Enterprise security plug-in as a default, and with LDAP and Windows Active Directory security plug-ins. Each security plug-in offers several key benefits.

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

The security plug-ins dynamically maintain third-party user and group listings. So, once you map an LDAP or Windows Active Directory group into BusinessObjects Enterprise, all users who belong to that group can log into BusinessObjects Enterprise. When you make subsequent changes to the third-party group membership, you need not update or refresh the listing.

BusinessObjects Enterprise supports the following security plug-ins:

- BusinessObjects Enterprise security plug-in
- LDAP security plug-in
- Windows AD and NT security plug-in

Note:

The third-party Windows NT, LDAP, and Windows AD security plug-ins work only once you have mapped groups from the external user database to BusinessObjects Enterprise.

Authentication and authorization

Authentication is the process of verifying the identity of a user who attempts to access the system. This process is distinct from authorization. Authorization is the process of verifying that the user has been granted sufficient rights to perform the requested action upon the specified object.

BusinessObjects Enterprise is fully customizable, therefore authentication processes can vary from system to system.

BusinessObjects Enterprise supports these methods of authentication:

- Enterprise authentication
- Windows NT authentication
- Lightweight Directory Access Protocol (LDAP) authentication
- Windows AD authentication

BusinessObjects Enterprise authentication

The system default, BusinessObjects Enterprise authentication, is used in environments that prefer to maintain a distinct set of accounts for use with BusinessObjects Enterprise.

BusinessObjects Enterprise authentication is always enabled; it cannot be disabled.

- Use the system default Enterprise Authentication if you prefer to create distinct accounts and groups for use with BusinessObjects Enterprise, or if you have not already set up a hierarchy of users and groups in a Windows NT server, an LDAP directory server, or a Windows AD server.

Windows NT authentication

BusinessObjects Enterprise supports NT authentication with the Windows NT security plug-in, which is included by default when the product is installed on Windows. Support for NT authentication means that users or groups created with NT, Windows 2000 and Windows 2003 can be used to

authenticate with BusinessObjects Enterprise. This allows you to map previously created NT user accounts and groups, instead of setting up each user and group within BusinessObjects Enterprise.

Note:

Although a user can configure Windows NT authentication for BusinessObjects Enterprise and custom applications through the CMC, the CMC and InfoView themselves do not support Windows NT authentication.

LDAP authentication

Lightweight Directory Access Protocol (LDAP) is a set of protocols used to access information stored in directories. A very common use for an LDAP directory is to maintain user and group account information.

BusinessObjects Enterprise supports the use of an existing LDAP account directory, eliminating the need to recreate user and group accounts in BusinessObjects Enterprise. By mapping your LDAP groups to BusinessObjects Enterprise, users are able to log into Enterprise with their LDAP user name and password.

Directories that support LDAP include:

- Sun iPlanet Directory Server
- Lotus Domino Directory Server
- IBM Secureway
- Novell Directory Services (NDS)

LDAP authentication is enabled using the Manage Authentication section of the CMC.

Note:

You can specify that BusinessObjects Enterprise use a Secure Sockets Layer (SSL) connection to communicate to the LDAP directory server for additional security. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Active Directory authentication

Windows AD security plug-in enables you to map user accounts and groups from your Windows 2000 Active Directory (AD) system to BusinessObjects Enterprise; it also enables BusinessObjects Enterprise to verify all login requests that specify Windows AD Authentication. Users are authenticated

against the Windows AD system, and have their membership in a mapped AD group verified before the Crystal Management Server (CMS) grants them an active BusinessObjects Enterprise session.

Note:

Although a user can configure Windows NT authentication for BusinessObjects Enterprise and custom applications through the CMC, the CMC and InfoView themselves do not support Windows AD authentication with NTLM. The only methods of authentication that the CMC and InfoView support are Windows AD with Kerberos, LDAP, Enterprise, and Trusted Authentication.

Trusted Authentication

Users prefer to log into the system once, without needing to provide passwords several times during a session. Trusted Authentication provides a Java single sign-on solution for integrating your BusinessObjects Enterprise authentication solution with third-party authentication solutions. Applications that have established trust with the Central Management Server can use Trusted Authentication to allow users to log on without providing their passwords. To enable Trusted Authentication, you must configure both the server, through the CMC, and the client, in the web.xml file. For more information, see BusinessObjects Enterprise Administrator's Guide.

Primary authentication

Primary authentication occurs when a user first attempts to access the system. One of two things can happen during primary authentication:

- If single sign-on is not configured, the user provides their credentials, such as their user name, password and authentication type. These details are entered by the users on the logon screen.
- If a method of single sign-on is configured, the credentials for the users are silently propagated. These details are extracted using other methods such as Kerberos and SiteMinder.

The authentication type may be Enterprise, Windows NT, LDAP, or Windows AD authentication, depending upon which type(s) you have enabled and set up in the Authentication management area of the Central Management Console (CMC). The user's web browser sends the information by HTTP to your web server, which routes the information to the CMS or the appropriate BusinessObjects Enterprise server.

Information Workflows

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

Authentication

Logging on to BusinessObjects Enterprise

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

Starting the Server Intelligence Agent

1. The Server Intelligence Agent (SIA) starts up and looks in the cache for a list of CMSes (local or remote) to connect to. This CMS list is kept up-to-date and refreshed as soon as a new CMS appears. According to

the information in the cache, the SIA either: (1) starts the local CMS and connects to it or (2) connects to a remote CMS.

2. After the SIA has successfully connected, it asks the CMS for a list of server service(s) to manage. The CMS finds information on server services and their configuration from the system database.
3. The system database returns the list of servers and the associated configuration information back to the CMS (for example, Adaptive Job Server, Destination Job Server, Desktop Intelligence Processing Server, and Crystal Reports Processing Server).
4. The CMS sends the list of servers and the configuration information to the SIA.
5. The SIA starts the servers (for example, Adaptive Job Server, Destination Job Server, Desktop Intelligence Processing Server, and Crystal Reports Processing Server) and begins monitoring them. The SIA starts the servers according to the associated configuration information.

Scheduling

Setting a schedule for a Crystal Report to run now

1. The user schedules a report and the request is sent to the web application server.
2. The web application server passes the request to the CMS.
3. The CMS determines whether or not the user has the appropriate rights to schedule the report.
4. If the user has the appropriate rights to schedule the report, the CMS commits the scheduled object request to the CMS system database.
5. When the scheduled time arrives, the CMS locates an available Crystal Reports Job Server based on the Maximum Jobs Allowed value configured for each Crystal Reports Job Server.
6. The CMS sends the job information to the Crystal Reports Job Server.
7. The Crystal Reports Job Server determines the location of the Input File Repository Server that houses this report. The Crystal Reports Job Server then requests the report template from the Input FRS.
8. The Input FRS locates the report template and then streams to the Crystal Reports Job Server.

9. The report template is placed in a temporary directory on the Crystal Reports Job Server.
10. The Crystal Reports Job Server launches a child process (JobServerChild.exe) to coordinate running the report.
11. JobServerChild.exe launches ProcReport.dll and passes it all instances received from the Crystal Reports Job Server. ProcReport.dll calls Crpe32.dll.
12. The report is created when the Crpe32.dll completes the following tasks:
 - Open the report.
 - Connect to the production database.
 - Process the report.
 - Create and save the report instance.
 - Pass the report back to JobServerChild.exe.
13. The Crystal Reports Job Server updates the CMS periodically with the job status. At this time the status shows that the report is processing.
14. JobServerChild.exe uploads the report instance to the Output FRS.
15. The Output FRS notifies the JobServerChild.exe that the report has been saved successfully.
16. JobServerChild.exe notifies the Crystal Reports Job Server that the report creation has completed.
17. The Report Job Server updates the CMS with the job status. The JobServerChild.exe clears itself from memory.
18. The CMS updates the job status in its memory, and then writes the instance information to the BusinessObjects Enterprise System database.

Running a schedule for a Crystal Report to a default location

1. The Central Management Server (CMS) constantly checks the system database to determine if there is any schedule to be run at that time.
2. When the time specified by the schedule arrives, the CMS locates an available Crystal Reports Job Server based on the Maximum Jobs Allowed value configured on each Crystal Reports Job Server. The CMS sends the job information to the Crystal Reports Job Server. The information the CMS sends to the Crystal Reports Job Server is Report ID, Format, Destination, Logon information, parameters, and selection formulas.

3. The Crystal Reports Job Server communicates with the Input File Repository Server (FRS) to obtain a report template as per the requested Report ID.
4. The Crystal Reports Job Server launches the JobChildserver process.
5. The child process (JobChildserver) launches the ProcReport.dll upon receiving the template from the Input File Repository Server via the Enterprise Infrastructure. The ProcReport.dll contains all of the parameters that were passed from the CMS to the Crystal Reports Job Server.
6. The ProcReport.dll launches the Crpe32.dll that processes the report according to all the parameters that were passed.
7. While still processing, records are retrieved from a database server as defined within a report.
8. The Crystal Reports Job Server updates the CMS periodically with the job status. At this time the status shows that it is processing.
9. Once the report is compiled into the memory of the Crystal Reports Job Server, it needs to be exported to a different format, such as Portable Document Format (PDF). When exporting to PDF, the PDF .dll is used.
10. The report with saved data also needs to be submitted to the default location. Then it will be sent to the Output FRS.
11. Once that process is finished, the Crystal Reports Job Server updates the CMS with the job status. At this time the status is reported as a success.
12. The CMS updates the job status in its memory, and then writes the instance information to the BusinessObjects Enterprise System database.

Setting a schedule for a Crystal Report

1. The web client submits a schedule request in an URL, typically via the web server to the web application server.
2. The web application server interprets the URL request and determines that the request is a schedule request. The web application server sends the schedule time, database login values, parameter values, destination, and format to the specified CMS.
3. The CMS ensures that the user has rights to schedule the object. If the user has sufficient rights, the CMS adds a new record to the system database. The CMS also adds the instance to its list of pending schedules.

Setting a schedule for a Web Intelligence document

1. The user sets a schedule for a document and the request is sent to the web server. The web server passes the document schedule request to the web application server.
2. The web application server passes the document schedule request to the CMS.
3. The CMS determines whether or not the user has the appropriate rights to schedule the document. If the user has the appropriate rights to schedule the document, the user then sets the different scheduling parameters, and the CMS commits the scheduled object request to the CMS system database. An instance of the Web Intelligence document is created in the CMS that contains all the relevant scheduling information.

Running a schedule for a Web Intelligence Document

1. The CMS monitors the system database to determine if there is a schedule run at that time.
2. When the scheduled time arrives, the CMS sends the schedule request and all the information about the request to the Adaptive Job Server that houses the Web Intelligence Scheduling and Publishing Service.
3. The Adaptive Job Server (Web Intelligence Scheduling and Publishing Service) locates an available Web Intelligence Processing Server based on the Maximum Jobs Allowed value configured on each Web Intelligence Processing Server.
4. The Web Intelligence Processing Server determines the location of the Input File Repository Server (FRS) that houses the document and the universe metalayer file on which the document is based. The Web Intelligence Processing Server then requests the document from the Input FRS. The Input FRS locates the Web Intelligence document as well as the universe file on which the document is based and then streams them to the Web Intelligence Processing Server.
5. The Web Intelligence document is placed in a temporary directory on the Web Intelligence Processing Server. The Web Intelligence Processing Server opens the document in memory. The QT.dll generates the SQL from the Universe on which the document is based. The Connection Server (component of the Web Intelligence Process Server) connects to the database. The query data passes through QT.dll back to the Document

Engine where the document is processed. A new successful instance is created.

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

Running a schedule for a program

1. The user schedules an object and the request is sent to the web server.
2. The web server passes the object schedule request to the web application server.
3. The web application server passes the request to the CMS.
4. The CMS determines if the user has the appropriate rights to schedule the object.
5. If the user has the appropriate rights to schedule the object, the CMS commits the scheduled object request to the CMS system database.
6. When the scheduled time arrives, the CMS locates an available Program Job Server based on the Maximum Jobs Allowed value configured on each Program Job Server.
7. The CMS sends the job information to the Program Job Server.
8. The Program Job Server communicates with the Input File Repository Server and requests the program object.
9. The Input File Repository Server returns the program object back to the Program Job Server.
10. The Program Job Server launches the scheduled object.
11. The Program Job Server updates the CMS periodically with the job status. At this time the status reported is that the program is processing.

12. The Program Job Server sends a log file to the Output File Repository Server.
13. The Output File Repository Server notifies the Program Job Server that the object was scheduled successfully by sending an object log file.
14. The Program Job Server updates the CMS with the job status.
15. The CMS updates the job status in its memory, and then writes the object instance information to the BusinessObjects Enterprise System database.

Sending an instance to a destination

1. The user schedules an object and the request is sent to the web server.
2. The web server passes the object schedule request to the web application server.
3. The web application server passes the request to the CMS.
4. The CMS determines if the user has the appropriate rights to schedule the object.
5. If the user has the appropriate rights to schedule the object, the CMS commits the scheduled object request to the CMS system database.
6. When the scheduled time arrives, the CMS locates an available Program Job Server based on the Maximum Jobs Allowed value configured on each Program Job Server.
7. The CMS sends the job information to the Program Job Server.
8. The Program Job Server communicates with the Input File Repository Server and requests the program object.
9. The Input File Repository Server returns the program object back to the Program Job Server.
10. The Program Job Server launches the scheduled object.
11. The Program Job Server updates the CMS periodically with the job status. At this time the status reported is that the program is processing.
12. The Program Job Server sends a log file to the Output File Repository Server.
13. The Output File Repository Server notifies the Program Job Server that the object was scheduled successfully by sending an object log file.
14. The Program Job Server updates the CMS with the job status.
15. The CMS updates the job status in its memory, and then writes the object instance information to the BusinessObjects Enterprise System database.

Viewing

Viewing an instance when the page exists on the Cache Server

1. The web client sends a view request in a URL to the web application server.
2. The web application server interprets the request and determines that it is a request to view the first page of the selected report instance. The web application server sends a request to the CMS to ensure that the user has rights to view the instance.
3. The CMS checks the system database to verify the user rights.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the instance.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the first page of the report instance. The Crystal Reports Cache Server checks to see if the page already exists. If the page does exist, the Crystal Reports Cache Server returns the page to the web application server.
6. The web application server sends the .epf page to the web client where it is rendered in the ActiveX viewer.

Viewing a page of a report instance when the cache file of the page does not exist

1. The user sends the view request through the web server to the web application server.
2. The web application server recognizes the request as a request to view a report page. The web application server checks the CMS to ensure the user has sufficient rights to view the report.
3. The CMS determines if the user has the appropriate rights to view the report.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the report.
5. The web application server sends a request to the Crystal Reports Cache Server for the requested report page (EPF file).

6. The Crystal Reports Cache Server determines if the requested EPF file exists in the cache directory.
7. The requested EPF file is not found in the cache directory.
8. The Crystal Reports Cache Server sends the request to the Crystal Reports Page Server.
9. The Crystal Reports Page Server queries the Output FRS for the requested report instance.
10. The Output FRS sends the requested report instance to the Crystal Reports Page Server.
11. The Crystal Reports Page Server opens the report instance and checks the report to determine if it has data.
12. The Crystal Reports Page Server determines that the report contains data and creates the .EPF file for the requested report page without having to connect to the production database.
13. The Crystal Reports Page Server sends the EPF file to the Crystal Reports Cache Server.
14. The Crystal Reports Cache Server writes the EPF file to the cache directory.
15. The Crystal Reports Cache Server sends the requested page to the web application server.
16. The web application server forwards the file to the web server.
17. The web server sends the requested page to the report viewer.

Viewing a Voyager workspace

1. The web client sends a request via the web server to the web application server to view a new workspace. The web client communicates with the web application server using DHTML AJAX technology (Asynchronous JavaScript and XML). The AJAX technology allows for partial page updates, so a new page does not have to be rendered for each new request.
2. The web application server translates the request and sends it to the platform (CMS) to determine whether a user is entitled to view or create a new workspace.
3. The CMS retrieves the user's credentials from the system database.
4. If the user is allowed to view or create a workspace, the CMS confirms this to the web application server. At the same time, it also sends a list of one or more available MDAS Servers via CORBA.

5. The web application server picks an MDAS Server from the list of available choices and sends a CORBA request to the MDAS Server to find the appropriate OLAP server(s) to create a new, or refresh an existing, workspace.
6. The MDAS server needs to communicate with the Input FRS to retrieve the appropriate workspace document that has information about the underlying OLAP Database and an initial OLAP query saved with it. The Input FRS retrieves the appropriate Information Analyzer workspace (.amw) from the underlying directory (via OS) and then streams that workspace back to the MDAS.
7. The MDAS Server opens the workspace, formulates a query, and sends it to the OLAP Database Server. The MDAS Server has to have an appropriate OLAP database client configured for the OLAP data source. The translation of the web client query into the appropriate OLAP query needs to occur. The OLAP Database Server sends the query result back to the MDAS Server.
8. The MDAS Server, based on the request to either create, view, print, or export, prerenders the result to enable the Java WAS to finish the rendering more quickly. The MDAS Server sends XML packages of prerendered result back to the web application server.
9. The web application server renders the workspace and sends the formatted page or portion of the page to the web client via the web server. The web client displays the updated or newly requested page. This is a zero-client solution that does not need to download any Java or ActiveX components.

On Demand

Viewing a report on demand

1. The web client sends the view on demand request in an URL typically via the web server to the web application server.
2. The web application server interprets the requested page and the values sent in the URL request and determines that it is a request to view the first page of the selected report object.
3. The web application server sends a request to the CMS to ensure that the user has rights to view the object. The CMS checks the system database to verify the user rights.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the object.

5. The web application server sends a request to the Crystal Reports Cache Server requesting the first page of the report object.
6. The Crystal Reports Cache Server checks to see if the page already exists. Unless the report meets the requirements for On Demand report sharing (within a set time of another On Demand request, database login, parameters), the Crystal Reports Cache Server sends a request for the Crystal Reports Processing Server to generate the page.
7. The Crystal Reports Processing Server requests the report object from the Input File Repository Server. The Input File Repository Server streams a copy of the object to the Crystal Reports Processing Server. The Crystal Reports Processing Server opens the report in its memory and checks to see if the report contains data.
8. Assuming that there is no data in the report object, the Crystal Reports Processing Server must connect to the database to query for data.
9. The Crystal Reports Processing Server sends the .epf page to the Crystal Reports Cache Server. The Crystal Reports Cache Server stores a copy of the .epf page in its cache directory in anticipation of new viewing requests.

Note:

An .etf page may also be generated and sent to the Crystal Reports Cache Server in this step. The .etf page (left pane group tree navigation of the report) is generated when the first page of report is generated and when the report is grouped. There is only one .etf page per report, but the size of this .etf page can be substantial.

10. The Crystal Reports Cache Server sends the .epf page to the web application server.
11. The web application server sends the .epf page to the web server. The web server sends the .epf page to the user's machine where it is rendered in the viewer in the web client.

Viewing a Web Intelligence document on demand

1. A web browser sends the view request to the web application server via the web server.
2. The web application server determines that the request is for a Web Intelligence document, and sends a request to the CMS to ensure the user has the appropriate rights to view the document.
3. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the document.

4. The web application server sends a request to the Web Intelligence Processing Server, requesting the document.
5. The Web Intelligence Processing Server requests the document from the Input File Repository Server as well as the universe file on which the requested document is built. The universe file contains metalayer information, including row- and column-level security.
6. The Input File Repository Server streams a copy of the document to the Web Intelligence Processing Server, as well as the universe file on which the requested document is built.
7. The Web Intelligence Report Engine opens the document in memory.
8. The Web Intelligence Report Engine uses QT component (inproc) and ConnectionServer (inproc). The QT component generates/validates/regenerates the SQL and connects to the database to run the query. The ConnectionServer uses the SQL to get the data from the database to the Report Engine where the document is processed.
9. The Web Intelligence Processing Server sends the viewable document page that was requested to the web application server. The web application server forwards this viewable page to the web server. The web server sends the viewable page to the user's machine, where it is rendered in a web browser.

Viewing a Desktop Intelligence document on demand using the web view format

1. The web client sends the view Desktop Intelligence document request in an URL to the web server.
2. The web server sends the request to the web application server.
3. The web application server interprets the requested page and the values sent in the URL request and determines it is a request to view a Desktop Intelligence document. The web application server sends a request to the CMS to ensure that the user has rights to view the document.
4. The CMS checks the system database to verify the user rights.
5. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the document.
6. The web application server sends a request to the Desktop Intelligence Cache Server requesting the document.
7. The Desktop Intelligence Cache Server checks whether the page is already cached. If it is, the Desktop Intelligence Cache Server returns that viewable page back to the web application server. If not, the Desktop Intelligence Cache Server asks the Desktop Intelligence Processing

Server to generate the requested viewable page of the Desktop Intelligence document.

8. The Desktop Intelligence Processing Server requests the document and the universe on which the document is based from the Input FRS. The Input FRS streams a copy of the document and the universe to the Desktop Intelligence Processing Server. The Desktop Intelligence report engine opens the document and the universe in its memory. The Desktop Intelligence Processing Server generates the SQL from the universe that the report is based on.
9. The Connection Server library (part of the Desktop Intelligence Processing Server) connects to the database to run the query. The query data is passed back to the report engine where the document is processed.
10. The Desktop Intelligence Processing Server sends the requested viewable page (HTML pages) of the document to the Desktop Intelligence Cache server.
11. The Desktop Intelligence Cache server stores that viewable page locally (HTML pages) in anticipation of future requests to view that already created page. The Desktop Intelligence Cache server then passes the viewable page (obtained from the Desktop Intelligence Processing Server) back to the web application server.
12. The web application server does not need to convert that viewable page to HTML because it is already in HTML format and passes the page to the web server.
13. The web server sends the HTML page (viewable page of the document) to the user's machine where it is rendered in the web browser.

Viewing a report on demand when the default view format is set to Web Java

1. The web client sends the view on demand request via the web server to the web application server.
2. The web application server interprets the requested page and the values sent in the URL request and determines that it is a request to view the first page of the selected report object.
3. The web application server sends a request to the CMS to ensure that the user has rights to view the object. The CMS checks the system database to verify the user rights.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the object.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the first page of the report object.

6. The Crystal Reports Cache Server checks to see if the page already exists. Unless the report meets the requirements for On Demand report sharing (within a set time of another On Demand request, database login, parameters), the Crystal Reports Cache Server sends a request for the Crystal Reports Processing Server to generate the page.
7. The Crystal Reports Processing Server requests the report object from the Input File Repository Server. The Input File Repository Server streams a copy of the object to the Crystal Reports Processing Server. The Crystal Reports Processing Server opens the report in its memory and checks to see if the report contains data.
8. Assuming that there is no data in the report object, the Crystal Reports Processing Server must connect to the database to query for data.
9. The Crystal Reports Processing Server sends the .epf page to the Crystal Reports Cache Server. The Crystal Reports Cache Server stores a copy of the .epf page in its cache directory in anticipation of new viewing requests. An .etf page may also be generated and sent to the Crystal Reports Cache Server in this step. The .etf page (left-pane group tree navigation of the report) is generated when the first page of the report is generated and when the report is grouped. There is only one .etf page per report, but the size of this .etf page can be substantial.
10. The Crystal Reports Cache Server sends the .epf page to the web application server.
11. The web application server sends the .epf page to the web server. The web server sends the .epf page to the user's machine where it is rendered in the viewer in the web client.



Security Concepts



3 chapter



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

Click the appropriate link to jump to that section:

- [Security overview](#)
- [Authentication and authorization](#)
- [Security plug-ins](#)
- [Active trust relationship](#)
- [Sessions and session tracking](#)
- [Environment protection](#)
- [Auditing web activity](#)

Security overview

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

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

Click the appropriate link to jump to that section:

- [Authentication and authorization](#)
- [Security plug-ins](#)
- [Active trust relationship](#)
- [Sessions and session tracking](#)
- [Environment protection](#)

- [Auditing web activity](#)
- For key procedures that show how to modify the default accounts, passwords, and other security settings, see *SAP BusinessObjects Enterprise Administrator's Guide*.
- For procedures that show how to set up authentication for Enterprise users, see *SAP BusinessObjects Enterprise Administrator's Guide*. For the basic information on how to set up third-party authentication to work with BusinessObjects Enterprise, see the following sections:
 - [Using NT Authentication](#)
 - [Using LDAP authentication](#)
 - [Using AD authentication](#)

Authentication and authorization

Authentication is the process of verifying the identity of a user who attempts to access the system, and authorization is the process of verifying that the user has been granted sufficient rights to perform the requested action upon the specified object.

This section describes the authentication and authorization processes in order to provide a general idea of how system security works within BusinessObjects Enterprise. Each of the components and key terms is discussed in greater detail later in this section. The detailed information on how to implement these different methods of authentication is discussed in the following section:

The current release supports these methods of authentication:

- Enterprise authentication
- Windows NT authentication
- LDAP authentication
- Windows AD authentication
- Trusted Authentication

If you want to use any of the third-party methods of authentication or Trusted Authentication, you will need to configure them before you use them.

Because BusinessObjects Enterprise is fully customizable, the authentication and authorization processes may vary from system to system. This section uses InfoView as a model and describes its default behavior. If you are developing your own BusinessObjects Enterprise end-user or administrative applications using the BusinessObjects Enterprise Software Development Kit (SDK), you can customize the system's behavior to meet your needs. For complete details, see the developer documentation available on your product CD.

Note:

Although a user can configure Windows NT authentication for BOE and custom applications through the CMC, the CMC and InfoView themselves do not support Windows NT authentication. The CMC and InfoView do not support Windows AD authentication with NTLM.

The only methods of authentication that the CMC and InfoView support are Windows AD with Kerberos, LDAP, Enterprise, and Trusted Authentication.

Related Topics

- [Using NT Authentication](#)
- [Using LDAP authentication](#)
- [Using AD authentication](#)

Primary authentication

Primary authentication occurs when a user first attempts to access the system. One of two things can happen during primary authentication:

- If single sign-on is not configured, the user provides their credentials, such as their user name, password and authentication type.

These details are entered by the users on the logon screen.

- If a method of single sign-on is configured, the credentials for the users are silently propagated.

These details are extracted using other methods such as Kerberos, SiteMinder.

- The authentication type may be Enterprise, Windows NT, LDAP, or Windows AD authentication, depending upon which type(s) you have enabled and set up in the Authentication management area of the Central

Management Console (CMC). The user's web browser sends the information by HTTP to your web server, which routes the information to the CMS or the appropriate BusinessObjects Enterprise server.

The web application server passes the user's information through a server-side script. Internally, this script communicates with the SDK and, ultimately, the appropriate security plug-in to authenticate the user against the user database.

For instance, if the user is logging on to InfoView and specifies Enterprise authentication, the SDK ensures that the BusinessObjects Enterprise security plug-in performs the authentication. The Central Management Server (CMS) uses the BusinessObjects Enterprise security plug-in to verify the user name and password against the system database. Alternatively, if the user specifies LDAP or Windows AD authentication, the SDK uses the corresponding security plug-in to authenticate the user.

If the security plug-in reports a successful match of credentials, the CMS grants the user an active system identity and the following actions are performed:

- The CMS creates an enterprise session for the user. While the session is active, this session consumes one user license on the system.
- The CMS generates and encodes a logon token and sends it to the web application server.
- The web application server stores the user's information in memory in a session variable. While active, this session stores information that allows BusinessObjects Enterprise to respond to the user's requests.

Note:

The session variable does not contain the user's password.

- The web application server keeps the logon token in a cookie on the client's browser. This is only used for failover purposes, such as when you have a clustered CMS or when InfoView is clustered for session affinity.

Note:

It is possible to disable the logon token. However, if you disable the logon token, you will disable failover.

Each of these steps contributes to the distributed security of BusinessObjects Enterprise, because each step consists of storing information that is used

for secondary identification and authorization purposes. This is the model used in InfoView. However, if you are developing your own client application and you prefer not to store session state on the web application server, you can design your application such that it avoids using session variables.

Note:

The third-party Windows NT, LDAP, and Windows AD security plug-ins work only once you have mapped groups from the external user database to BusinessObjects Enterprise. For procedural details, see the following sections:

- [Using AD authentication with NTLM](#)
- [Using LDAP authentication](#)
- [Using NT Authentication](#)

Note:

In a single sign-on situation, BusinessObjects Enterprise retrieves users' credentials and group information directly from Windows AD or SiteMinder. Hence, users are not prompted for their credentials.

Single sign-on support

The term single sign-on is used to describe different scenarios. At its most basic level, it refers to a situation where a user can access two or more applications or systems while providing their log-on credentials only once, thus making it easier for users to interact with the system.

Single sign-on to the InfoView and the CMC can be provided by BusinessObjects Enterprise, or by different authentication tools depending on your application server type and operating system.

These methods of single sign-on are available if you are using a Java application server on Windows:

- Windows AD with Kerberos
- Windows AD with SiteMinder.

These methods of single sign-on are available if you are using IIS on Windows:

- Windows AD with Kerberos.

- Windows AD with NTLM
- Windows AD with SiteMinder.

These methods of single sign-on support is available on Windows or Unix, with either any supported web application server for the platform.

- LDAP with SiteMinder.
- Trusted Authentication.
- Windows AD with Kerberos

Note:

Windows AD with Kerberos is supported if the Java application is on UNIX. However, the BusinessObjects Enterprise services need to run on a Windows server.

The following table describes the methods of single sign-on support for the InfoView and CMC that are available.

Authen- tication Mode	CMS Server	Options	Notes
Win- dows AD	Win- dows only	Windows AD with Kerberos only.	Windows AD authentication to the InfoView and CMC is available out of the box.
LDAP	Any sup- ported platform	Supported LDAP di- rectory servers, with SiteMinder only.	LDAP authentication to the In- foView and CMC is available out of the box. SSO to the InfoView and CMC requires SiteMinder.
Enter- prise	Any sup- ported platform	Trusted Authentica- tion	Enterprise authentication to the InfoView and CMC is available out of the box. SSO with enter- prise authentication to the In- foView and CMC requires Trusted Authentication.

Note:

Single sign-on using Windows NT authentication is not supported for the InfoView or the CMC.

Within the context of BusinessObjects Enterprise, we distinguish the following levels of single sign-on:

- *Single sign-on to BusinessObjects Enterprise*
- *Single sign-on to database*
- *End-to-end single sign-on*

Single sign-on to BusinessObjects Enterprise

Single sign-on to BusinessObjects Enterprise means that once users have logged on to the operating system (for Windows) or SiteMinder protected resources (for LDAP), they can access BusinessObjects Enterprise applications that support SSO without having to provide their credentials again. When a user logs on, a security context for that user is created. This

context can be propagated to BusinessObjects Enterprise in order to perform SSO - resulting in the user being logged on as a BusinessObjects Enterprise user that corresponds to the user.

The term “anonymous single sign-on” also refers to single sign-on to BusinessObjects Enterprise, but it specifically refers to the single sign-on functionality for the Guest user account. When the Guest user account is enabled, which it is by default, anyone can log on to BusinessObjects Enterprise as Guest and will have access to BusinessObjects Enterprise. For more information, see the Managing Accounts and Groups chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

For information on configuring single sign-on to BusinessObjects Enterprise with LDAP authentication, see [Configuring LDAP authentication](#).

Single sign-on to database

Once users are logged on to BusinessObjects Enterprise, single sign-on to the database enables them to perform actions that require database access, in particular, viewing and refreshing reports, without having to provide their logon credentials again. Single sign-on to the database can be combined with single sign-on to BusinessObjects Enterprise, to provide users with even easier access to the resources they need. See [End-to-end single sign-on](#).

In BusinessObjects Enterprise XI, single sign-on to the database is supported through Windows AD using Kerberos. You may want to use single sign-on to the database rather than end-to-end single sign-on, if you don't want the account for IIS to be trusted for delegation.

See these sections for information on configuring single sign-on to the database with BusinessObjects Enterprise:

- [Using AD authentication with Kerberos](#)
- [Configuring Kerberos and single sign-on to the database for Java application servers](#)
- [Configuring Kerberos and single sign-on for Java InfoView](#).

End-to-end single sign-on

End-to-end single sign-on refers to a configuration where users have both single sign-on access to BusinessObjects Enterprise at the front-end, and single sign-on access to the databases at the back-end. Thus, users need to provide their logon credentials only once, when they log on to the operating system, to have access to BusinessObjects Enterprise and to be able to perform actions that require database access, such as viewing reports.

In BusinessObjects Enterprise XI end-to-end single sign-on is supported through Windows AD and Kerberos.

Related Topics

- [Using AD authentication with Kerberos](#)

Security plug-ins

Security plug-ins expand and customize the ways in which BusinessObjects Enterprise authenticates users. BusinessObjects Enterprise currently ships with the system default BusinessObjects Enterprise security plug-in together with the Windows NT, LDAP, and Windows AD security plug-ins.

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

The security plug-ins dynamically maintain third-party user and group listings. Once you map a Windows NT, LDAP, or Windows AD group into BusinessObjects Enterprise, all users who belong to that group can successfully log on to BusinessObjects Enterprise. When you make subsequent changes to the third-party group membership, you do not need to update or refresh the listing in BusinessObjects Enterprise. For instance, if you map a Windows NT group to BusinessObjects Enterprise, and then you add a new NT user to the NT group, the security plug-in dynamically creates an alias for that new user when he or she first logs on to BusinessObjects Enterprise with valid NT credentials.

Moreover, security plug-ins enable you to assign rights to users and groups in a consistent manner, because the mapped users and groups are treated as if they were Enterprise accounts. For example, you might map some user accounts or groups from Windows NT, and some from an LDAP directory server. Then, when you need to assign rights or create new, custom groups within BusinessObjects Enterprise, you make all of your settings in the CMC.

Each security plug-in acts as an authentication provider that verifies user credentials against the appropriate user database. When users log on to BusinessObjects Enterprise, they choose from the available authentication types that you have enabled and set up in the Authorization management area of the CMC: Enterprise (the system default), Windows NT, LDAP, or Windows AD.

Note:

The Windows NT and Windows AD security plug-ins cannot authenticate users if the BusinessObjects Enterprise server components are running on UNIX.

BusinessObjects Enterprise security plug-in

The BusinessObjects Enterprise security plug-in (`secEnterprise.dll`) is installed and enabled by default when you install BusinessObjects Enterprise. This plug-in allows you to create and maintain user accounts and groups within BusinessObjects Enterprise; it also enables the system to verify all logon requests that specify Enterprise authentication. In this case, user names and passwords are authenticated against the BusinessObjects Enterprise user list, and users are allowed or disallowed access to the system based solely on that information. For details on setting up Enterprise users and groups, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Default accounts

When you first install BusinessObjects Enterprise, this plug-in sets up two default Enterprise accounts: Administrator and Guest. Neither account has a default password.

Single sign-on

The BusinessObjects Enterprise authentication provider supports anonymous single sign-on for the Guest account. Thus, when users connect to BusinessObjects Enterprise without specifying a user name and password,

the system logs them on automatically under the Guest account. If you assign a secure password to the Guest account, or if you disable the Guest account entirely, you disable this default behavior. For details, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Processing extensions

BusinessObjects Enterprise offers you the ability to further secure your reporting environment through the use of customized processing extensions. A processing extension is a dynamically loaded library of code that applies business logic to particular BusinessObjects Enterprise view or schedule requests before they are processed by the system.

Through its support for processing extensions, the BusinessObjects Enterprise administration SDK essentially exposes a "handle" that allows developers to intercept the request. Developers can then append selection formulas to the request before the report is processed.

A typical example is a report-processing extension that enforces row-level security. This type of security restricts data access by row within one or more database tables. The developer writes a dynamically loaded library that intercepts view or schedule requests for a report (before the requests are processed by a Job Server, Processing Server, or Report Application Server). The developer's code first determines the user who owns the processing job; then it looks up the user's data-access privileges in a third-party system. The code then generates and appends a record selection formula to the report in order to limit the data returned from the database. In this case, the processing extension serves as a way to incorporate customized row-level security into the BusinessObjects Enterprise environment.

Tip:

In BusinessObjects Enterprise XI, you can also set and enforce row-level security through the use of Business Views. For more information, see the *Business Views Administrator's Guide*.

By enabling processing extensions, you configure the appropriate BusinessObjects Enterprise server components to dynamically load your processing extensions at runtime. Included in the SDK is a fully documented API that developers can use to write processing extensions. For more information, see the developer documentation available on your product distribution.

Note:

In the current release, processing extensions can be applied only to Crystal report (.rpt) objects.

Active trust relationship

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

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

Logon tokens

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

- **Number of minutes**

This attribute restricts the lifetime of the logon token.

- **Number of logons**

This attribute restricts the number of times that the logon token can be used to log on to BusinessObjects Enterprise.

Both attributes hinder malicious users from gaining unauthorized access to BusinessObjects Enterprise with logon tokens retrieved from legitimate users.

Note:

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

When the logon cookie has been disabled, and the web server or web browser times out, the user is presented with the logon screen. When the cookie is enabled, and the server or browser times out, the user is seamlessly logged back onto the system. However, because state information is tied to the web session, the user's state is lost. For example, if the user had a navigation tree expanded and a particular item selected, the tree is reset.

For BusinessObjects Enterprise, the default is to have logon tokens enabled in the web client, however, you can disable logon tokens for InfoView. When you disable the logon tokens in the client, the user session will be limited by the web server or web browser timeout. When that session expires, the user will be required to log in again to BusinessObjects Enterprise.

Ticket mechanism for distributed security

Enterprise systems dedicated to serving a large number of users typically require some form of distributed security. An enterprise system may require distributed security to support features such the transfer of trust (the ability to allow another component to act on behalf of the user)

BusinessObjects Enterprise addresses distributed security by implementing a ticket mechanism (one that is similar to the Kerberos ticket mechanism). The CMS grants tickets that authorize components to perform actions on behalf of a particular user. In BusinessObjects Enterprise, the ticket is referred to as the logon token.

This logon token is most commonly used over the Web. When a user is first authenticated by BusinessObjects Enterprise, he or she receives a logon token from the CMS. The user's web browser caches this logon token. When the user makes a new request, other BusinessObjects Enterprise components can read the logon token from the user's web browser.

Sessions and session tracking

In general, a session is a client-server connection that enables the exchange of information between the two computers. A session's state is a set of data that describes the session's attributes, its configuration, or its content. When you establish a client-server connection over the Web, the nature of HTTP limits the duration of each session to a single page of information; thus, your web browser retains the state of each session in memory only for as long as any single Web page is displayed. As soon as you move from one web page to another, the state of the first session is discarded and replaced with the state of the next session. Consequently, Web sites and Web applications must somehow store the state of one session if they need to reuse its information in another.

BusinessObjects Enterprise uses two common methods to store session state:

- **Cookies**—A cookie is a small text file that stores session state on the client side: the user's web browser caches the cookie for later use. The BusinessObjects Enterprise login token is an example of this method.
- **Session variables**—A session variable is a portion of memory that stores session state on the server side. When BusinessObjects Enterprise grants a user an active identity on the system, information such as the user's authentication type is stored in a session variable. So long as the session is maintained, the system neither has to prompt the user for the information a second time nor has to repeat any task that is necessary for the completion of the next request.

For Java deployments, the session is used to handle .jsp requests; for .NET deployments, the session is used to handle .aspx requests.

Note:

Ideally, the system should preserve the session variable while the user is active on the system. And, to ensure security and to minimize resource usage, the system should destroy the session variable as soon as the user has finished working on the system. However, because the interaction between a web browser and a web server can be stateless, it can be difficult to know when users leave the system, if they do not log off explicitly. To address this issue, BusinessObjects Enterprise implements session tracking.

Related Topics

- [CMS session tracking](#)

CMS session tracking

The CMS implements a simple tracking algorithm. When a user logs on, the user is granted a CMS session, which the CMS preserves until the user logs off, or until the web application server session variable is released.

The web application server session is designed to notify the CMS on a recurring basis that it is still active, so the CMS session is retained so long as the web application server session exists. If the web application server session fails to communicate with the CMS for a ten-minute time period, the CMS destroys the CMS session. This handles scenarios where client-side components shut down irregularly.

Environment protection

Environment protection refers to the security of the overall environment in which client and server components communicate. Although the Internet and web-based systems are increasingly popular due to their flexibility and range of functionality, they operate in an environment that can be difficult to secure. When you deploy BusinessObjects Enterprise, environment protection is divided into two areas of communication:

- *Web browser to web server*
- *Web server to BusinessObjects Enterprise*

Web browser to web server

When data is transmitted between the web browser and the web server, some degree of security is usually required. Relevant security measures usually involve two general tasks:

- Ensuring that the communication of data is secure.
- Ensuring that only valid users retrieve information from the web server.

Note:

These tasks are typically handled by web servers through various security mechanisms, including the Secure Sockets Layer (SSL) protocol, Windows NT Challenge/Response authentication, and other such mechanisms. It is

good practice to use Secure Sockets Layer (SSL) to reduce security risk between the browser and application or web server. For procedural information, see [Configuring servers for SSL](#).

You must secure communication between the web browser and the web server independently of BusinessObjects Enterprise. For details on securing client connections, refer to your web server documentation.

Web server to BusinessObjects Enterprise

Firewalls are commonly used to secure the area of communication between the web server and the rest of the corporate intranet (including BusinessObjects Enterprise). BusinessObjects Enterprise supports firewalls that use IP filtering or static network address translation (NAT). Supported environments can involve multiple firewalls, web servers, or application servers.

For complete details on BusinessObjects Enterprise and firewall interaction, see [Understanding communication between BusinessObjects Enterprise components](#).

Auditing web activity

BusinessObjects Enterprise provides insight into your system by recording web activity and allowing you to inspect and to monitor the details. The web application server allows you to select the web attributes—such as time, date, IP address, port number, and so on—that you want to record. The auditing data is logged to disk and stored in comma-delimited text files, so you can easily report off the data or import it into other applications.

Protection against malicious logon attempts

No matter how secure a system is, there is often at least one location that is vulnerable to attack: the location where users connect to the system. It is nearly impossible to protect this location completely, because the process of simply guessing a valid user name and password remains a viable way to attempt to "crack" the system.

BusinessObjects Enterprise implements several techniques to reduce the probability of a malicious user achieving access to the system. The various restrictions listed below apply only to Enterprise accounts—that is, the restrictions do not apply to accounts that you have mapped to an external user database (Windows NT, LDAP, or Windows AD). Generally, however, your external system will enable you to place similar restrictions on the external accounts.

Click the appropriate link to jump to that section:

- [Password restrictions](#)
- [Logon restrictions](#)
- [User restrictions](#)
- [Guest account restrictions](#)

Password restrictions

Password restrictions ensure that Enterprise users create passwords that are relatively complex. You can enable the following options:

- Enforce mixed-case passwords

This option ensures that passwords contain at least two of the following character classes: upper case letters, lower case letters, numbers, or punctuation.

- Must contain at least N characters

By enforcing a minimum complexity for passwords, you decrease a malicious user's chances of simply guessing a valid user's password.

Logon restrictions

Logon restrictions serve primarily to prevent dictionary attacks (a method whereby a malicious user obtains a valid user name and attempts to learn the corresponding password by trying every word in a dictionary). With the speed of modern hardware, malicious programs can guess millions of passwords per minute. To prevent dictionary attacks, BusinessObjects Enterprise has an internal mechanism that enforces a time delay (0.5–1.0

second) between logon attempts. In addition, BusinessObjects Enterprise provides several customizable options that you can use to reduce the risk of a dictionary attack:

- Disable accounts after N failed attempts to log on
- Reset failed logon count after N minute(s)
- Re-enable account after N minute(s)

User restrictions

User restrictions ensure that Enterprise users create new passwords on a regular basis. You can enable the following options:

- Must change password every N day(s)
- Cannot reuse the N most recent password(s)
- Must wait N minute(s) to change password

These options are useful in a number of ways. Firstly, any malicious user attempting a dictionary attack will have to recommence every time passwords change. And, because password changes are based on each user's first logon time, the malicious user cannot easily determine when any particular password will change. Additionally, even if a malicious user does guess or otherwise obtain another user's credentials, they are valid only for a limited time.

Guest account restrictions

The BusinessObjects Enterprise authentication provider supports anonymous single sign-on for the Guest account. Thus, when users connect to BusinessObjects Enterprise without specifying a user name and password, the system logs them on automatically under the Guest account. If you assign a secure password to the Guest account, or if you disable the Guest account entirely, you disable this default behavior. For details, see the *SAP BusinessObjects Enterprise Administrator's Guide*.



Managing Licenses

4

chapter



Overview

This section shows you how to use the CMC to manage license information for your BusinessObjects Enterprise deployment. It includes information on:

- [Adding a license key](#)
- [Viewing current account activity](#)

Managing license information

The License Keys area identifies the number of concurrent, named, and processor licenses associated with each key.

To view license information

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 Licensing Information area. To purchase additional license keys:

- Contact your Business Objects sales representative.
- Contact your regional office. For details, go to:

http://www.businessobjects.com/company/contact_us/

Adding a license key

Note:

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.

To add a license key

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

Note:

Key codes are case-sensitive.

3. Click **Add.**

The key is added to the list.

Viewing current account activity

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.



Managing and Configuring Servers



5

chapter



Server management overview

Tip:

For the latest version of this documentation, consult the *SAP BusinessObjects Enterprise XI Administrator's Guide*. The latest version of this guide is available on the Business Objects web site: http://support.businessobjects.com/documentation/product_guides/default.asp

The following table provides definitions for important concept used throughout this section.

Concept	Definition used
Service	A subsystem that provides a function. For example the Destination Configuration service is used to configure target recipients for Crystal for Crystal Reports.
Server	An OS level process hosting one or more services. Examples include the Central Management Server (CMS) and Adaptive Processing Server. The Adaptive Processing Server can host the "Client Auditing Proxy Service", "Publishing Service", "Search Service", etc.
Node	A collection of BusinessObjects Enterprise servers, all running on the same host and managed by a single SIA. One or more nodes can be on a single host.
Host	A physical computer or a virtual machine.
Server Intelligence Agent (SIA)	A SIA is deployed on every node. It starts, stops, monitors and manages all servers on its node. If a server crashes or ceases to function, the SIA will restart the server.

This section provides information on a range of server tasks that allow you to customize the behavior of BusinessObjects Enterprise. It also includes information on the server settings that you can alter to accommodate the needs of your organization. The default values for these settings have been chosen to maximize the reliability, predictability, and consistency of operation of a typical BusinessObjects Enterprise installation. The default settings ensure the highest degree of data accuracy and timeliness. For example, by default, data sharing between reports is disabled. When running reports on demand, disabling data sharing means that every user can always assume that they will receive the latest data.

If you prefer to place more emphasis on the efficiency, economy, and scalability of BusinessObjects Enterprise, you can tune server settings to set your own balance between system reliability and performance. For example, enabling data sharing between reports markedly increases system performance when user loads are heavy. To take advantage of this feature while ensuring that every user receives data that meets your criteria for timeliness, you can also specify how long data will be shared between users.

BusinessObjects Enterprise administrative tools

BusinessObjects Enterprise includes two key administrative tools that allow you to access a variety of server settings:

- **Central Management Console (CMC)**

The CMC is the web-based administration tool that allows you to view and to modify server settings while BusinessObjects Enterprise is running. For instance, you use the CMC to change the status of a server, change server settings, access server metrics, or create server groups. Because the CMC is a web-based interface, you can configure your BusinessObjects Enterprise servers remotely over the Internet or through your corporate intranet.

For more information about the Servers management area of the CMC, see [Working with the Servers management area in the CMC](#).

- **Central Configuration Manager (CCM)**

The CCM is a troubleshooting tool that allows you to configure and manage the Server Intelligence Agent. The Server Intelligence Agent is the component that allows you to manage all servers through the CMC. You can also use the CCM to create and manage nodes in your deployment. Note that most server management tasks are now handled through the CMC, not in the CCM. (The CCM was the primary tool for server management in previous versions.) After you configure and enable nodes in the CCM, you can perform other server management tasks in the CMC. For more information, see [About Server Intelligence](#).

The CCM is now used primarily for node configuration, and for troubleshooting when you cannot access the CMC. For example, if you need to reconfigure the CMS and do not have access to the CMC, you can click Manage Servers in the CCM to log in and view all servers in

your deployment. For more information, see [Starting, stopping, and restarting servers](#).

When managing servers through the Central Configuration Manager (CCM) in a side-by-side deployment, where two BusinessObjects Enterprise systems work alongside one another, you must ensure that you connect to the correct deployment so that you don't accidentally edit, disable, or delete the servers connected to another system. It is recommended that you follow these best practices:

- Specify the port number when connecting to the deployments.

For example, mymachine:6400 or mymachine:6403.

- Administer the BusinessObjects Enterprise deployment from the local machine, and administer the previous version's deployment remotely, from a different machine.
- Use different passwords for the administrator accounts for the two deployments.

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 BusinessObjects Enterprise. 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.

Navigation tree option	Description
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. For more information, see Server groups .
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. For more information, see Working with nodes .

Navigation tree option	Description
<p>Service Categories</p>	<p>Provides a list of the types of services that may be in your deployment. Service categories are divided into core BusinessObjects Enterprise services and services associated with specific Business Objects components. Service categories include:</p> <ul style="list-style-type: none"> • Core Services • Crystal Reports • Desktop Intelligence • Performance Management • Voyager • Web Intelligence • Excelsius <p>Select a service category in the navigation list to view the servers in the category.</p>

Navigation tree option	Description
Server Status	<p>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:</p> <ul style="list-style-type: none"> • Stopped • Starting • Initializing • Running • Stopping • Started with Errors • Failed • Waiting for resources <p>For more information about changing the state of a server, see Viewing and changing the status of servers.</p>

About the Details pane

Depending on which options you have selected in the navigation tree, the Details pane on the right side of the Servers management area shows a list of servers, server groups, states, categories, or nodes. The following table describes the information listed for servers in the Details pane.

Note:

For nodes, server groups, categories, and states, the Details pane usually shows names and descriptions.

Details pane column	Description
Server Name or Name	Displays the name of the server.
State	<p>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:</p> <ul style="list-style-type: none"> • Stopped • Starting • Initializing • Running • Stopping • Started with Errors • Failed • Waiting for resources <p>For more information about changing the state of a server, see Viewing and changing the status of servers.</p>
Enabled	Displays whether the server is enabled or disabled.
Stale	<p>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 dialog box, you may need to restart the server before the changes will take effect. For information on restarting servers, see Starting, stopping, and restarting servers.</p>

Details pane column	Description
Kind	Displays the type of server.
Host Name	Displays the Host Name for the server.
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. For more information, see To change a server's properties .
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.

About Web Application Container Servers

Web Application Container Servers (WACS) can be used to host BusinessObjects Enterprise web applications such as the Central Management Console (CMC) on Windows operating systems. WACS requires a minimum effort to install, maintain, and configure, and provide an administrative interface that is consistent with other BusinessObjects Enterprise servers.

Related Topics

- [Web Application Container Server \(WACS\)](#)

About Server Intelligence

Server Intelligence is the underlying server management architecture that simplifies the administration and deployment of BusinessObjects Enterprise servers and services. Instead of manually administering servers via the Central Configuration Manager, you can now handle most server administration tasks online using the Central Management Console.

Server Intelligence allows you to use the CMC for all daily maintenance tasks, such as adding and configuring new servers, or starting and stopping existing servers. And it also allows you to automate certain server processes, such as restarting or shutting down servers that stop unexpectedly. If a CMS system database becomes unavailable, it is automatically reconnected. Server Intelligence also manages server configuration information, storing it in the CMS so you can easily restore default server settings or create duplicate "clone" servers with the same settings. All of these features make it easier to fine-tune your system's performance and fault tolerance.

Note:

Server Intelligence simplifies many procedures that you needed to perform manually in earlier versions of BusinessObjects Enterprise. Many of the tasks that used to be carried out in the CCM are now managed in the CMC. To understand the differences in these procedures, experienced administrators should carefully read the new server management procedures in this section.

About the Server Intelligence Agent (SIA)

Server Intelligence is managed via the Server Intelligence Agent (SIA), the component that processes the server management tasks. An SIA is deployed on each node within your BusinessObjects Enterprise deployment. A node is a collection of BusinessObjects Enterprise servers, running on the same host and managed by a single SIA.

The SIA maintains server status according to the settings you specify in the CMC. It processes the CMC's requests to start, stop, monitor, and manage all servers on the node, and it also monitors potential problems and automatically restarts servers that have shut down unexpectedly. The SIA ensures optimal performance by continually monitoring server status information, which is stored in the CMS database. When you change a

server's settings or add a new server in the CMC, the CMS notifies the SIA, and the SIA performs the task.

The SIA is automatically configured during installation, but you can change these default settings through the CCM.

Server management: what's new in this version of BusinessObjects Enterprise

This section summarizes the key differences in server management tasks between BusinessObjects Enterprise XI Release 2 and BusinessObjects Enterprise XI 3.x. One of the key improvements in this version of BusinessObjects Enterprise is that most server management tasks are now handled through the CMC instead of the CCM. Although this change makes servers easier to manage, administrators who are accustomed to using earlier versions of BusinessObjects Enterprise will notice several changes in how many common tasks are performed.

Most of the procedural changes are the result of the introduction of Server Intelligence, a new feature that allows you to handle most server management tasks via the CMC. For general information about Server Intelligence, see [About Server Intelligence](#).

The following table provides a list of some of the procedures that are affected by the introduction of Server Intelligence, and links are included for the new step procedures:

Procedure	BusinessObjects Enterprise XIR2	BusinessObjects Enterprise XI 3.x
Adding a new machine with a CMS to a cluster.	Performed an Expand installation.	You can perform a Custom installation. During the Custom installation, make sure you select the CMS and deselect the database installation option.

Procedure	BusinessObjects Enterprise XIR2	BusinessObjects Enterprise XI 3.x
Viewing or changing a server's state.	The server's state was displayed in the CCM and the CMC, but only the CMC allowed you to change server states on any machine in the cluster. The CCM could manage servers only on one machine at a time .	<p>You can now use either the CMC or the CCM to view and change the state of servers located on any machine in the cluster.</p> <p>In the CMC, you can now use the Server Status option in the navigation tree to view servers according to their current state.</p> <p>In the CMC, you can now use the Server Status option in the navigation tree to view servers according to their current state. (In the CCM, click Manage Servers button to log in and view all servers from your deployment.)</p>
Adding or deleting a server	Servers were added and deleted in the CCM.	You can now add and delete servers in the CMC. For more information, see Adding, cloning, and deleting servers .

Procedure	BusinessObjects Enterprise XIR2	BusinessObjects Enterprise XI 3.x
Adding a new machine to a cluster	<p>Performed a standalone installation and used a copy of destination cluster CMS database to verify that everything worked fine on the new machine. In the CCM, the CMS was pointed to a new cluster's CMS database and other configuration changes were made to account for this change. For example, for an Oracle CMS database, you changed the database information in the tns.ora file and changed all database references from <code>-ns oldCMS</code> to <code>-ns newCMS</code>.</p>	<p>You can use the Custom installation to add a new machine to a cluster.</p> <p>If testing can be performed after adding a new machine, then you can add it via the CMC. For more information, see Adding, cloning, and deleting servers. If no down time is allowed, perform a standalone installation and move node or server information from one deployment to another. For more information, see To import nodes from one cluster to another.</p>
Changing the OS account or password for BusinessObjects Enterprise servers	<p>Selected the servers one by one in the CCM, and for each server updated the password or account</p>	<p>In the CCM, select the node on which the servers runs, then update the password or account</p>

Procedure	BusinessObjects Enterprise XIR2	BusinessObjects Enterprise XI 3.x
Clustering two machines together during installation.	Performed an Expand installation.	Perform a Custom installation. During the Custom installation, make sure you select the CMS and deselect the database installation option.
Configuring for a firewall using static port binding	In the CCM, you added <code>-port</code> and <code>-request port</code> options to the server's command line.	Double-click the server in the CMC to view and change the port settings. For more information, see Configuring port numbers .
Configuring for a multi-homed deployment	In the CCM, you added <code>-port</code> and <code>-request port</code> options to the server's command line.	Double-click the server in the CMC to view and change the port settings. For more information, see Configuring port numbers .

Working with nodes

A node is a collection of BusinessObjects Enterprise servers, all running on the same host and managed by a single Server Intelligence Agent (SIA). The SIA monitors the servers on the node and ensures they are running properly. For more information about the SIA, see [About the Server Intelligence Agent \(SIA\)](#).

Nodes are a new feature in this version of BusinessObjects Enterprise. In previous versions, servers were associated with a particular machine. Now

that servers are organized by node, it is much easier to transfer servers and configuration settings between machines. You can also have multiple nodes on a single host.

You can use nodes to cluster servers together. You may want to organize your servers on multiple nodes depending on how you plan to manage your servers. For example, if you want to be able to start and stop the CMS without affecting other servers, you'll want to store it on a separate node.

Note:

You can have one or more nodes on the same machine. Multiple nodes allow you to run processes under different OS user accounts. (All servers on each node run under the same OS user account.)

For more information about clustering, see [Clustering Central Management Servers](#).

To add a node

Nodes are initially created by the installation setup program during installation, but you can also add additional nodes. To create a new node on a new machine, you can perform a Custom installation. On a machine where BusinessObjects Enterprise is installed, you can create a new node using the CCM. This procedure describes how to add a node from the CCM. For more information about Custom installations, please consult the *SAP BusinessObjects Enterprise Installation Guide*. Once you have added a node, use the CCM to configure the node's database information. This is important if a CMS is managed by the new node. Failure to configure this information could cause the system to fail.

Note:

To recreate a SIA that already exists in the CMS system database, see [Recreating a Server Intelligence Agent on a local machine](#).

1. In the CCM, click **Add Server Intelligence Agent**.

Note:

The same procedure is used for creating a node and for creating a new Server Intelligence Agent. You cannot have one without the other.

2. In the "Server Intelligence Agent Wizard", provide a name and port number for the new Server Intelligence Agent (SIA).

Note:

The node name cannot be changed after you create it.

3. Choose whether or not you want to install default servers with the new node by selecting or deselecting **Create default servers on the new node**.
 - Deselect this check box if you do not want to install the default servers. For example, you may plan to clone servers onto the new node from an existing deployment. For more information about cloning, see [Cloning servers](#).
 - Select this check box if you want to install all new default servers.

Note:

- This option only creates servers for which binaries already exist on the target machine, and this does not necessarily reflect all possible BusinessObjects Enterprise servers.
 - If you need to remove default servers after the node has already been created, see [To remove servers from a new node](#).
4. Make sure that the **Recreate Server Intelligence Agent on the local host if it already exists in the CMS system database** check box is not selected.
 5. Click **Next**.
 6. Provide the CMS port number and CMS system database name.

Note:

- In order to add a new SIA on a deployed system, a CMS must be running.
 - If you are planning to use auditing features then you should also provide information about your auditing database.
7. Provide your connection information for the CMS database, then click **Next**.

The Server Intelligence Agent Wizard creates a new node with its own Server Intelligence Agent. Information about the new node is added to the CMS system database you selected. The new node automatically includes all default BusinessObjects Enterprise services.

Note:

You can have one or more nodes on the same machine. Multiple nodes allow you to run processes under different OS user accounts. All servers on each node would run under the same OS user account.

Tip:

Once you have added a node, use the CCM to configure the node's database information. This is very important if a CMS will ever be managed by the node.

To remove servers from a new node

When you create a new node, you can choose whether to create default servers or not. If you choose to create default servers, the node will be automatically populated with all default servers. If you do not want to include the default servers, make sure the **Create default servers on the new node** button is not selected when you create the node. However, if you want to remove some of the default servers after you have already created the node, use the following procedure. For more information about adding and deleting servers, see [Adding, cloning, and deleting servers](#).

1. After you create a new node, do not start the Server Intelligence Agent (SIA) for the node. If necessary, stop the SIA.

Note:

For information on adding nodes, see [To add a node](#).

2. Go to the "Servers" management area of the CMC.
3. In the navigation tree, select the new node.
The list of servers in the node appear on the right.
4. Disable the servers you want to remove.
For more information, see [Enabling and disabling servers](#).
5. Stop the servers you want to remove.
6. Delete the servers you want to remove.
For more information on deleting servers, see [Deleting a server](#).

Recreating a Server Intelligence Agent on a local machine

You can recreate a Server Intelligence Agent (SIA) on a local machine if it already exists in the CMS system database. (This is also known as "adopting"

a node.) You should recreate a Server Intelligence Agent only in serious situations; for example, if a machine hosting BusinessObjects Enterprise servers is lost, damaged, or has failed and you need to recreate the node on the new machine replacement. You can recreate only nodes that do not exist on any physical machines in your deployment. (Make sure that no other machines host the same node.)

Note:

Be very careful when recreating a SIA. If performed incorrectly, this procedure may cause port conflicts. Do not recreate a SIA on a live system. Before you recreate the node, you should first install BusinessObjects Enterprise on the machine. If you are performing a Custom installation, make sure that you install all servers that used to be on this node.

To recreate a Server Intelligence Agent on a local machine

This procedure is used to add a node and Server Intelligence Agent to a local machine when the SIA already exists in the CMS system database. You may want to use this procedure if you are replacing a machine with BusinessObjects Enterprise servers.

Note:

Although BusinessObjects Enterprise allows you to have nodes on different operating systems, recreating nodes is supported only for servers that are using the same operating system. For example, BusinessObjects Enterprise does not support recreating a Server Intelligence Agent on a Solaris machine when the original SIA that exists in the CMS system database was on a Windows machine.

1. In the CCM, click **Add Server Intelligence Agent**.

Note:

The same procedure is used for creating a node and for creating a new Server Intelligence Agent. You cannot have one without the other.

2. In the "Server Intelligence Agent Wizard", provide a name and port number for the new Server Intelligence Agent (SIA).
3. Select the **Create default servers on the new node** check box, then click **Next**.

Note:

This option only creates servers for which binaries already exist on the target machine, and this does not necessarily reflect all possible BusinessObjects Enterprise servers.

4. Provide the CMS port number and CMS system database name for the inactive cluster, then click **Next**.

Note:

If you are using auditing, you can also provide information about your system's auditing database.

5. Select the **Recreate Server Intelligence Agent on the local host if it already exists in the CMS system database** check box.
6. Provide your connection information for the CMS database, then click **Next**.

The setup program creates a new node on the inactive cluster. Information about the new node is added to the CMS system database you selected.

Viewing and changing the status of servers

The status of a server is its current state of operation: a server can be running, starting, stopping, stopped, failed, initializing, enabled, disabled, or waiting for resources. To respond to BusinessObjects Enterprise requests, a server must be running and enabled. A server that is disabled is still running as a process; however, it is not accepting requests from the rest of BusinessObjects Enterprise. A server that is stopped is no longer running as a process.

This section shows how to modify the status of servers by using the CMC.

Related Topics

- [To view a server's status](#)
- [Starting, stopping, and restarting servers](#)
- [Enabling and disabling servers](#)
- [Stopping a Central Management Server](#)
- [To start a server automatically](#)

To view a server's status

1. Go to the "Servers" management area of the CMC.

The **Servers List** includes a **State** column that provides the status for each server in the list.

2. If you want to view a list of all of the servers that currently have a particular status, expand the **Server Status** option in the navigation tree and select the status you want.

A list of servers with the selected status appears in the Details pane.

Note:

This can be particularly useful if you need to quickly view a list of servers that are not starting properly or have stopped unexpectedly.

Starting, stopping, and restarting servers

Starting, stopping, and restarting servers are common actions that you perform when you configure servers or take them offline for other reasons. For example, if you want to change the name of a server, then you must first stop the server. Once you have made your changes, you start the server again to effect your changes. If you make changes to a server's configuration settings, the CMC will prompt you if you need to restart the server.

The remainder of this section tells you when a certain configuration change requires that you first stop or restart the server. However, because these tasks appear frequently, the concepts and differences are explained first, and the general procedures are provided for reference.

Action	Description
Stopping a server	You may need to stop BusinessObjects Enterprise servers before you can modify certain properties and settings.

Action	Description
Starting a server	If you have stopped a server to configure it, you need to start it to effect your changes and to have the server resume processing requests.
Restarting a server	Restarting a server is a shortcut to stopping a server completely and then starting it again. If you need to restart a server after changing a server setting, you will be prompted by the CMC.
Starting a server automatically	You can set servers to start automatically when the Server Intelligence Agent starts.
Force Termination	Stops a server immediately (whereas when you stop a server, it will stop when it has completed its current processing activities).

Tip:

When you stop (or restart) a server, you terminate the server's process, thereby stopping the server completely. If you want to prevent a server from receiving requests without actually stopping the server process, you can also disable servers. We recommend that you disable servers before stopping them so that they can finish processing any jobs they have in progress. For details, see [Enabling and disabling servers](#).

To start, stop, or restart servers with CMC

1. Go to the "Servers" management area of the CMC.

A list of servers appears. For each server, the CMC provides information about the server's state and whether or not the server is enabled. Possible states include: **Initializing**, **Starting**, **Running**, **Enabled**, **Disabled**, **Stopping**, **Stopped**, **Failed**, and **Waiting for resources**.

Note:

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. For more information about server states, see [Viewing and changing the status of servers](#).

2. Select the server whose status you want to change.
3. Depending on the action you need to perform, click **Start**, **Stop**, or **Restart**.

Note:

You can also choose these commands from the **Action** menu.

4. Click **Refresh** to update the page.

To start, stop, or restart a Windows server with the CCM

1. In the CCM, click the **Manage Servers** button.
2. Log into the CMS.
3. In the "Manage Servers" dialog box, select the server that you want to start, stop, or restart.
4. Click **Start**, **Stop**, or **Restart**.
5. Click **Close** to return to the CCM.

Note:

In previous versions of BusinessObjects Enterprise, the CCM was the primary tool for managing servers.

To start, stop, or restart a UNIX server with the CCM

Use the `ccm.sh` script. For reference, see the Unix Tools chapter.

To start a server automatically

Note:

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

1. Go to the **Servers** management area of the CMC.
2. Select the server you want to start automatically, then choose **Properties** from the **Manage** menu.
3. In the Properties dialog box, select the **Automatically start this server when the Server Intelligence Agent starts** check box, then click **OK**.

Note:

If the automatic start setting is deselected for all CMSs in the cluster, you need to use the CCM to restart the system. Right-click the SIA, choose Properties. On the Startup tab, change the Autostart setting to Yes, then click Save. Restart the SIA.

Stopping a Central Management Server

If your BusinessObjects Enterprise installation has more than one active Central Management Server (CMS), you can shut down a single CMS without losing data or affecting system functionality. Another CMS on the node will assume the workload of the stopped server. Clustering multiple CMSs enables you to perform maintenance on each of your Central Management Servers in turn without taking BusinessObjects Enterprise out of service.

However, if your BusinessObjects Enterprise deployment has a single CMS, shutting it down will make BusinessObjects Enterprise unavailable to your users and will interrupt the processing of reports and programs. To avoid this problem, the Server Intelligence Agent for each node ensures that at least one CMS is running at all times. You can still stop a CMS by stopping its SIA, but before stopping the SIA, you should disable the processing servers via the CMC so that they can finish any jobs in progress before BusinessObjects Enterprise shuts down, because all other servers on the node will also shut down.

Note:

You may encounter situations where the CMS has been stopped and you need to restart the system from the CCM. For example, if you shut down all of the CMSs on a node and all of the CMSs are not set to automatically start when the SIA starts, then you need to use the CCM to restart the system. In the CCM, right-click the SIA and choose Properties. On the Startup tab, change the Autostart setting to Yes, then click Save. Restart the SIA.

If you want to configure your system so that you can start and stop a Central Management Server without starting and stopping other servers, you have two options:

- For all of the other servers on the node, clear the selection of the **Automatically start this server when the Server Intelligence Agent starts** check box. You can edit this setting in the **Servers** management area of the CMC. Select the server, choose **Properties** from the **Manage** menu and then clear the check box.
- Put the CMS on a separate node. Create a new node and clone the CMS to the node. With the CMS on its own node, you can easily shut down the node without affecting other servers. For more information about creating nodes, see [Working with nodes](#). For information about cloning servers, see [Cloning servers](#).

See [Viewing and changing the status of servers](#) for general information about changing server status in the CMC.

For more information on node clusters, see [Clustering Central Management Servers](#).

Enabling and disabling servers

When you disable a BusinessObjects Enterprise server, you prevent it from receiving and responding to new BusinessObjects Enterprise requests, but you do not actually stop the server process. This is especially useful when you want to allow a server to finish processing all of its current requests before you stop it completely.

For example, you may want to stop a Job Server before rebooting the machine it is running on. However, you want to allow the server to fulfill any outstanding report requests that are in its queue. First, you disable the Job Server so it cannot accept any additional requests. Next, go to the Central

Management Console to monitor when the server completes the jobs it has in progress. (From the Servers management area, choose the server name and then the metrics tab). Then, once it has finished processing current requests, you can safely stop the server.

Note:

- The CMS must be running in order for you to enable and/or disable other servers.
- A CMS cannot be enabled or disabled.

To enable and disable servers with CMC

1. Go to the "Servers" management area of the CMC.
2. Select the server whose status you want to change.
3. Depending on the action you need to perform, click **Enable** or **Disable**.

To enable or disable a Windows server with the CCM

1. In the CCM, click **Manage Servers**.
2. When prompted, log on to your CMS with the credentials that provide you with administrative privileges to BusinessObjects Enterprise.
3. In the "Manage Servers" dialog box, select the server that you want to enable or disable.
4. Click **Enable** or **Disable**.
5. Click **OK** to return to the CCM.

To enable or disable a UNIX server with the CCM

Use the `ccm.sh` script. For reference, see the Unix Tools chapter.

Adding, cloning, and deleting servers

Tip:

If you want to add new hardware to BusinessObjects Enterprise by installing server components on new, additional machines, run the BusinessObjects Enterprise installation and setup program from your product distribution. The setup program allows you to perform an Custom installation. During the

Custom installation, specify the CMS from your existing deployment, and select the components that you want to install on the local machine. For details on custom installation options, see the *SAP BusinessObjects Enterprise Installation Guide*.

Adding a server

These steps add a new instance of a server to the local machine. You can run multiple instances of the same BusinessObjects Enterprise server on the same machine.

To add a server

1. In the CMC, go to the "Servers" management area.
2. On the **Manage** menu, click **New**, then click **New Server**.
The "Create New Server" dialog box appears.
3. Choose the **Service Category**.
4. Choose a type of server from the **Select Service** list, then click **Next**.
5. To add an additional service to the server, select the service in the **Available Additional Services** list and click **>**.

Note:

Additional services are not available for all server types.

6. After adding the additional services you want, click **Next**.
7. If your BusinessObjects Enterprise 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. 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 automatically.

Note:

- For more information about configuring individual servers, see [Configuring server settings](#).
- To change the default port numbers for the server, see [Configuring port numbers](#).

11. Use the CMC to start and enable the new server when you want it to begin responding to BusinessObjects Enterprise requests.

Note:

For details, see [Viewing and changing the status of servers](#).

Cloning servers

BusinessObjects Enterprise XI 3.x allows you to clone servers. In previous versions of BusinessObjects Enterprise, you had to create a new server instance and then configure all of the settings for that server. Now, if you want to add a new server instance, you can clone an existing server. The cloned server retains the configuration settings of the original server. This can be particularly useful if you are expanding your deployment and want to create new server instances that use almost all of the same server configuration settings as an existing server.

Cloning also simplifies the process of moving servers between nodes. If you want to move an existing CMS to another node, you can clone it to the new node. The cloned CMS appears on the new node and retains all of the configuration settings of the original CMS.

There are some special considerations to keep in mind when cloning servers. You may not want all settings to be cloned, so it's good practice to check the cloned server to make sure it meets your needs. For example, if you clone a CMS, make sure you change the port number settings that were copied from the original CMS to the cloned CMS.

Note:

- Before you clone servers, make sure that all machines in your deployment have the same version of BusinessObjects Enterprise (and any patches if applicable).

- You can clone servers existing on different or the same machines. However, you can clone servers only to machines where the required binaries for the server are installed.
- When you clone a server, it does not necessarily mean that the new server will use the same OS credentials. The user account is controlled by the Server Intelligence Agent that the server is running under.

Using placeholders for server settings

Server setting placeholders are listed on a dedicated page in the Central Management Console (CMC). When you double-click any server listed under "Servers" in the CMC, a link is provided on the left-hand navigation pane for "Placeholders". The "Placeholders" page lists all the available placeholder names and their associated values for the selected server. Placeholders contain read-only values and the placeholder names begin and end with the percentage character %.

Note:

You can always overwrite a placeholder setting with a specific string in the CMC Server "Properties" page.

Example:

Placeholders are useful when cloning servers. For example, multi-drive machine A has BusinessObjects Enterprise installed on D:\Program Files\Business Objects\BusinessObjects Enterprise 12.0. So the %DefaultAuditingDir% placeholder will be D:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Auditing\.

On another machine, machine B, there is only one disc drive (no drive D) and BusinessObjects Enterprise is installed on C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0. In this case the %DefaultAuditingDir% placeholder will be C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Auditing\.

To clone the Event Server from machine A to machine B, if placeholders are used for the Auditing Temporary Directory, the placeholders will resolve themselves and the Event Server will work properly. If no placeholders are used, the Event Server will fail unless you manually overwrite the Auditing Temporary Directory setting.

To clone a server

1. On the machine you want to add the cloned server, log onto the CMC.
2. In the CMC, choose **Servers** from the navigation list.
3. On the **Actions** menu, click **Clone Server**.
 The "Clone Server" dialog box appears.
4. In the "Clone Server" dialog box, type a name for the server (or use the default name) in the **New Server Name** 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 on the **Servers** list in the "Servers" management area of the CMC.

Note:

Port number settings are also cloned. In many cases, such as cloning a CMS, you will want to change the port number to avoid port conflicts between the original server and its clone.

Deleting a server

These steps delete an instance of a server.

To delete a server

1. Go to the "Servers" management area of the CMC.

Note:

For information on stopping servers, see [Starting, stopping, and restarting servers](#).

2. Stop the server that you want to delete.
3. Select the server and choose **Delete** from the **Manage** menu.
4. When prompted for confirmation, click **OK**.

Server groups

Server groups provide a way of organizing your BusinessObjects Enterprise servers to make them easier to manage. That is, when you manage a group of servers, you need only view a subset of all the servers on your system. More importantly, server groups are a powerful way of customizing BusinessObjects Enterprise to optimize your system for users in different locations, or for objects of different types.

If you group your servers by region, you can easily set up default processing settings, recurrent schedules, and schedule destinations that are appropriate to users who work in a particular regional office. You can associate an object with a single server group, so the object is always processed by the same servers. And you can associate scheduled objects with a particular server group to ensure that scheduled objects are sent to the correct printers, file servers, and so on. Thus, server groups prove especially useful when maintaining systems that span multiple locations and multiple time zones.

If you group your servers by type, you can configure objects to be processed by servers that have been optimized for those objects. For example, processing servers need to communicate frequently with the database containing data for published reports. Placing processing servers close to the database server that they need to access improves system performance and minimizes network traffic. Therefore, if you had a number of reports that ran against a DB2 database, you might want to create a group of Processing Servers that process reports only against the DB2 database server. If you then configured the appropriate reports to always use this Processing Server group for viewing, you would optimize system performance for viewing these reports.

After creating server groups, configure objects to use specific server groups for scheduling, or for viewing and modifying reports. Use the navigation tree in the Servers management area of the CMC to view server groups. The Server Groups List option displays a list of server groups in the details pane, and the Server Groups option allows you to view the servers in the group.

Creating a server group

To create a server group, you need to specify the name and description of the group, and then add servers to the group.

To create a server group

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. Use the **Description** field to include additional information about the group.
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 the > arrow.

Tip:

Use CTRL+click to select multiple servers.

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. For more information, see [Viewing and changing the status of servers](#).

Working with server subgroups

Subgroups of servers provide you with a way of further organizing your servers. A subgroup is just a server group that is a member of another server group.

For example, if you group servers by region and by country, then each regional group becomes a subgroup of a country group. To organize servers in this way, first create a group for each region, and add the appropriate servers to each regional group. Then, create a group for each country, and add each regional group to the corresponding country group.

There are two ways to set up subgroups: you can modify the subgroups of a server group, or you can make one server group a member of another. The results are the same, so use whichever method proves most convenient.

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 the > arrow.

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.

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.
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 the > arrow.

Tip:

Use CTRL+click to select multiple server groups.

5. Click **OK**.

Modifying the group membership of a server

You can modify a server's group membership to quickly add the server to (or remove it from) any group or subgroup that you have already created on the system.

For example, suppose that you created server groups for a number of regions. You might want to use a single Central Management Server (CMS) for multiple regions. Instead of having to add the CMS individually to each regional server group, you can click the server's "Member of" link to add it to all three regions at once.

To modify a server's group membership

1. Go to the "Servers" management area of the CMC.
2. Locate the server whose membership information you want to change.
3. Choose **Properties** from the **Manage** menu.
4. In the "Properties" dialog box, click **Existing Server Groups** in the navigation list.

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.

5. To change the groups that the server is a member of, use the arrows to move server groups between the lists, then click **OK**.

User access to servers and server groups

You can use rights to grant people access to servers and server groups, allowing them to perform tasks such as starting and stopping servers.

Depending on your system configuration and security concerns, you may want to limit server management to the BusinessObjects Enterprise administrator. However, you may need to provide access to other people using those servers. Many organizations have a group of IT professionals dedicated to server management. If your server team needs to perform regular server maintenance tasks that require them to shut down and start up servers, you need to grant them rights to the servers. You may also want

to delegate BusinessObjects Enterprise server administration tasks to other people. Or you may want different groups within your organization to have control over their own server management.

To grant access to a server or server group

1. Go to the "Servers" management area of the CMC.
2. Select the server or server group you want to grant access to.
3. Choose **Properties** from the **Manage** menu.
4. In the "Properties" dialog box, click **User Security**.
5. Click **Add Principals** to add users or groups that you want to give access to the selected server or server group.

The "Add Principals" dialog box appears.

6. Select the user or group you want to grant access to the specified server or server group, then click **>**.
7. Click **OK**.
8. In the "Assign Security" dialog box, choose the security settings you want for the user or group.

For detailed information about assigning rights, refer to the Setting Rights chapter.

Object rights for the Report Application Server

To allow users to create or modify reports over the Web through the Report Application Server (RAS), you must have RAS Report Modification licenses available on your system. You must also grant users a minimum set of object rights. When you grant users these rights to a report object, they can select the report as a data source for a new report or modify the report directly:

- View objects (or "View document instances" as appropriate)
- Edit objects
- Refresh the report's data
- Export the report's data

User must also have permission to add objects to at least one folder before they can save new reports back to BusinessObjects Enterprise.

To ensure that users retain the ability to perform additional reporting tasks (such as copying, scheduling, printing, and so on), it's recommended that you first assign the appropriate access level and update your changes. Then, change the access level to Advanced, and add any of the required rights that are not already granted. For instance, if users already have View On Demand rights to a report object, you allow them to modify the report by changing the access level to Advanced and explicitly granting the additional Edit objects right.

When users view reports through the Advanced DHTML viewer and the RAS, the View access level is sufficient to display the report, but View On Demand is required to actually use the advanced search features. The extra Edit objects right is not required.

Configuring server settings

This section includes technical information and procedures that show how you can modify settings for BusinessObjects Enterprise servers.

The majority of the settings discussed in this section allow you to integrate BusinessObjects Enterprise more effectively with your current hardware, software, and network configurations. Consequently, the settings that you choose will depend largely upon your own requirements.

Most of the following procedures involve making changes in a server's Properties dialog box in the CMC. It is important to note that not all changes occur immediately. If a setting cannot change immediately, the Properties dialog box displays 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.

Note:

This section does not show how to configure your Web application server to deploy BusinessObjects Enterprise applications. This task is typically performed when you install BusinessObjects Enterprise. For details, see the *SAP BusinessObjects Enterprise Installation Guide*.

Related Topics

- [To change a server's properties](#)
- [Changing the connect port used by Tomcat](#)

- *Configuring port numbers*
- *Copying data from one CMS system database to another*
- *Deleting and recreating the CMS system database*
- *Selecting a new or existing CMS database*
- *Setting root directories and idle times of the File Repository Servers*
- *Modifying performance settings*
- *Configuring destinations for job servers*
- *Configuring Windows processing servers for your data source*
- *Configuring UNIX processing servers for your data source*

To change a server's properties

1. Go to the "Servers" management area of the CMC.
2. Select the server whose settings you want to change.
3. Choose **Properties** from the **Manage** menu.
4. Make the changes you want, then click **Save** or **Save & Close**.

Note:

Not all changes occur immediately. If a setting cannot change immediately, the Properties dialog box displays 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.

Working with configuration templates

Configuration templates allow you to easily configure multiple instances of servers. Configuration templates store a list of settings for each service type, which you can use to configure additional server instances. For example, if you have a dozen Web Intelligence Processing Servers that you want to configure identically, you only need to configure settings for one of them. You can then use the configured service to define the configuration template for Web Intelligence Processing Servers, and then apply the template to the other 11 service instances.

Each type of BusinessObjects Enterprise service has its own configuration template. For example, there is one configuration template for the Web Intelligence Processing service type, one for the Publishing service type, and so on. The configuration template is defined in the server properties in the Central Management Console (CMC).

When you make a server use a configuration template, existing settings for the server are overwritten with the values from the template and lost. If you later decide to stop using the template, the original settings are not restored. Subsequent changes to the configuration template no longer affect the server.

It is good practice to use configuration templates as follows:

1. Set the configuration template on one server. For information, see [To set a configuration template](#).
2. Assuming you want the same configuration on all servers of the same type, check **Use Configuration Template** for all servers of the same type, including the one where you set the configuration template. For information, see [To apply a configuration template to a server](#).
3. Later, if you want to change the configuration of all services of this type, view the properties of any one of the services, deselect the **Use Configuration Template** check box. Change the settings you want, then select **Set Configuration Template** for this server and click **Save**. All services of that type are updated. By not having a server that is always set as the configuration template, you ensure that you will not accidentally change configuration settings for all servers of that type.

To set a configuration template

You can set a configuration template for each type of service. You cannot set multiple configuration templates for one type of 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. Select the server that hosts services whose configuration template you want to set.
3. Choose **Properties** from the **Manage** menu.

Note:

You can also double-click the server to open its "Properties" page.

4. 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.

Note:

If you don't explicitly define the settings for the configuration template, the service's default settings are used.

5. To apply the configuration template to other services of the same type, proceed to [To apply a configuration template to a server](#).
6. If you need to restore the original default settings for the service, see [To restore system defaults](#).

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. For more information, see [To set a configuration template](#).

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. Select the server that is hosting a service you want to apply the configuration template to.
3. Choose **Properties** from the **Manage** menu.

Note:

You can also double-click the server to open its "Properties" page.

4. Select the **Use Configuration Template** check box and click **Save** or **Save & Close**.

Note:

If the server requires you to restart it in order for the new settings to take effect, it will show up as "stale" in the servers list.

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.

For information about setting the configuration template, see [To set a configuration template](#).

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. Select the server hosting a service that you want to restore system defaults for.
3. Choose **Properties** from the **Manage** menu.

Note:

You can also double-click the server to open its "Properties" page.

4. Select the **Restore System Defaults** check box and click **Save** or **Save & Close**.

The original factory default settings for the particular service type are restored.

Configuring server network settings

The networking settings for BusinessObjects Enterprise servers are managed through the CMC. These settings are divided into two categories: port settings and host identification.

Default settings

During installation, server host identifiers are set to **Auto assign**. Each server can however be assigned either a specific IP address or a hostname. The default CMS port number is 6400. The other BusinessObjects Enterprise servers dynamically bind to available ports. Port numbers are automatically managed by BusinessObjects Enterprise, but you can use the CMC to specify port numbers

Network environment options

BusinessObjects Enterprise supports both Internet Protocol 6 (IPv6) and Internet Protocol version 4 (IPv4) network traffic. You can use BusinessObjects server and client components in any of the following environments :

- IPv4 network: all server and client components run with IPv4 protocol only.
- IPv6 network: all server and client components run with IPv6 protocol only.
- Mixed IPv6/IPv4 network: server and client components can run with both IPv6 and IPv4 protocols.

Note:

Network configuration should be performed by the system and network administrator. BusinessObjects Enterprise does not provide a mechanism to designate a networking environment. You can use the CMC to bind to a specific IPv6 or IPv4 IP address for any of your BusinessObjects Enterprise servers.

Mixed IPv6/IPv4 environment

The IPv6/IPv4 networking environment enables the following :

- BusinessObjects Enterprise servers can service both IPv6 and IPv4 requests when running in mixed IPv6/IPv4 mode.
- Client components can interoperate with servers as IPv6-only nodes, IPv4-only nodes, or IPv6/IPv4 nodes.

The mixed mode is particularly useful in the following scenarios:

- You are moving from an IPv4-only node to an IPv6-only node environment. All the client and server components will continue to seamlessly

interoperate until the transition is complete. You can then deactivate the IPv4 settings for all the servers.

- Third party software that is not IPv6 compatible will continue to function in the IPv6/IPv4 node environment.

Note:

DNS names do not resolve properly if IPv6-only node is used with Windows 2003. It is recommended that your deployment runs as both IPv6/IPv4 if IPv4 stack is disabled on Windows 2003.

Server host identification options

Host identification options can be specified in the CMC for every BusinessObjects Enterprise server. The following table summarizes the options available in the Common Settings area:

Option	Description
Auto assign	<p>This is the default setting for all servers. When Auto-Assign is selected, the server automatically binds the server's Request Port onto the first network interface on the machine.</p> <p>Note: It is good practice to select the Auto-Assign checkbox for the Host Name setting. However in some cases, such as when the server is running on multi-homed machine, or when the server needs to inter-operate with a certain firewall configuration, you should consider using either a specific hostname or IP address. For more information see Configuring a multihomed machine and the "Working with Firewalls" chapter in the <i>SAP BusinessObjects Enterprise Administrator's Guide</i>.</p>
Hostname	Specifies the host name of the network interface that the server listens for requests on. For the CMS, this setting specifies the host name of the network interface that the CMS binds the Name Server Port and the Request Port.
IP Address	Specifies the IP address of the network interface that the server listens for requests on. For the CMS this setting specifies the address of the network interface that the CMS binds the Name Server Port and the Request Port. For every server, separate fields are provided to specify IPv4 and/or IPv6 IP addresses.

Note:

Important: If you specify **Auto-Assign** on multi-homes machines, the CMS may automatically bind to the wrong network interface. To prevent this from happening, make sure the network interfaces on the host machine are listed in the correct order (using the machine's OS tools). You must also specify the Host Name setting for the CMS in the CMC. For more information, see [To troubleshoot multiple network interfaces](#).

Note:

If you are working with multihomed machines or in certain NAT firewall configurations, you may need to specify the Host Name using fully qualified domain names instead of host names. For details, see [Configuring a multihomed machine](#) or the "Working with Firewalls" chapter.

To modify a server's host identification

1. Go to the "Servers" management area of the CMC.
2. Select the server, then choose **Stop Server** from the **Actions** menu.
3. Choose **Properties** from the **Manage** menu.
4. Under **Common Settings**, select one of the following options:

Option	Description
Auto assign	The server will bind to one of the available network interfaces.
Hostname	Enter the host name of the network interface on which server listens for requests.
IP Address	Enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface on which server listens for requests. Note: To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

5. Click **Save** or **Save & Close**.
The changes are reflected in the command line displayed on the "Properties" tab.
6. Start and enable the server.

Configuring a multihomed machine

A multihomed machine is one that has multiple network addresses. You may accomplish this with multiple network interfaces, each with one or more IP addresses, or with a single network interface that has been assigned multiple IP addresses.

If you have multiple network interfaces, each with a single IP address, change the binding order so that the network interface at the top of the binding order is the one you want the BusinessObjects Enterprise servers to bind to. If your interface has multiple IP addresses, use the Host Name option in the CMC to specify a network interface card for the BusinessObjects Enterprise server. It can be specified by host name or IP address. For more information

about configuring the Host Name setting, see [To troubleshoot multiple network interfaces](#).

Tip:

This section shows how to restrict all servers to the same network address, but it is possible to bind individual servers to different addresses. For instance, you might want to bind the File Repository Servers to a private address that is not routable from users' machines. Advanced configurations such as this require your DNS configuration to route communications effectively between all the BusinessObjects Enterprise server components. In this example, the DNS must route communications from the other BusinessObjects Enterprise servers to the private address of the File Repository Servers.

Configuring the CMS to bind to a network address

Note:

On a multi-homed machine, the Host Identifier can be set to the fully qualified domain name or the IP address of the interface that you want the server to bind to.

To configure the CMS to bind to a network address

1. Go to the **Servers** management area of the CMC.
2. Select the CMS and choose **Properties** from the **Manage** menu.
3. Under "Common Settings", select one of the following options:
 - Hostname: enter the host name of the network interface to which the server will bind.
 - IP Address: enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface to which the server will bind.

Note:

To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

Caution:

Do not select Auto assign.

4. For **Request Port** you can do one of the following:
 - Select the **Auto assign** option.
 - Enter a valid port number in the field provided.
5. Make sure that a port number is specified in the Name Server Port dialog box.

Note:

The default port number is 6400.

Configuring the remaining servers to bind to a network address

The remaining BusinessObjects Enterprise servers select their ports dynamically by default. For information on disabling the Auto assign setting that dynamically propagates this information, see [To change the port a server uses for accepting requests](#).

To troubleshoot multiple network interfaces

On a multi-homed machine, the CMS may automatically bind to the wrong network interface. To prevent this from happening, you can ensure the network interfaces on the host machine are listed in the correct order (using the machine's OS tools), or make sure you specify the Host Name setting for the CMS in the CMC. If the primary network interface is not routable, you can use the following procedure to configure BusinessObjects Enterprise to bind to a non-primary routable network interface. Perform these steps immediately after installing BusinessObjects Enterprise on the local machine, before you install BusinessObjects Enterprise on other machines.

1. Open the CCM and stop the SIA for the node on the machine that has multiple network interfaces.
2. Right-click the SIA and choose **Properties**.
3. In the "Properties" dialog box, click the "Configuration" tab.
4. To bind the SIA to a specific network interface, type in the **Port** field one of the following:
 - the hostname of the target network interface and port number (use the hostname:port number format)
 - the IP address of the target network interface and port number (use the IP address:port number format)
5. Click **OK** and select the "Startup" tab.
6. From the "Local CMS Servers" list select the CMS and click **Properties**.
7. To bind the CMS to a specific network interface, type in the **Port** field one of the following:
 - the hostname of the target network interface and port number (use the hostname:port number format)
 - the IP address of the target network interface and port number (use the IP address:port number format)

8. Click **OK** to apply the new settings.
9. Start the SIA and wait for the servers to start.
10. Launch the Central Management Console (CMC), and go to the "Servers" management area. Repeat steps 11-14 for each server.
11. Select the server, then choose **Stop Server** from the **Actions** menu.
12. Choose **Properties** from the **Manage** menu.
13. Under **Common Settings**, select one of the following options:
 - Hostname: enter the host name of the network interface to which the server will bind.
 - IP Address: enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface to which the server will bind.

Note:

To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

Caution:

Do not select Auto assign.

14. Click **Save** or **Save & Close**.
15. Return to the CCM and restart the SIA.

The SIA restarts all servers on the node. All servers on the machine now bind to the correct network interface.

Configuring port numbers

During installation, the CMS is set up to use default port numbers. The default CMS port number is 6400. This port falls within the range of ports reserved by Business Objects (6400 to 6410). BusinessObjects Enterprise communication on these ports should not conflict with third-party applications.

When started and enabled, each of the other BusinessObjects Enterprise servers dynamically binds to an available port (higher than 1024), registers with this port on the CMS, and then listens for BusinessObjects Enterprise requests. If necessary, you can instruct each server component to listen on a specific port (rather than dynamically selecting any available port).

Port numbers can be specified on each server's Properties tab in the CMC. This table summarizes the options under the "Common Settings" area as they relate to port usage for specific server types:

Setting	CMS	Other Servers
Request Port	Specifies the port that the CMS uses for accepting all requests from other servers (except for Name Server requests). Uses the same network interface as the Name Server Port. When Auto assign is selected, the server automatically uses an OS-assigned port number.	Specifies the port on which the server listens for all requests. When Auto assign is selected, the server automatically uses a port number assigned by the OS.
Name Server Port	Specifies the BusinessObjects Enterprise port on which the CMS listens for name service requests. The default is 6400.	Not applicable.

To change the default CMS port in the CMC

If there is a CMS already running on the cluster, you can use the CMC to change the default CMS port number.

1. Go to the "Servers" management area of the CMC.
2. Double-click the CMS in the server list.
3. Replace the **Name Server Port** number with the port that you want the CMS to listen on. (The default port is 6400.)

Note:

- The CMS uses the same network interface card for the request port and the name server port.
 - The settings you choose on the Properties page are reflected in the server command line, which also appears on the Properties page.
4. Click **Save & Close**.
 5. Restart the CMS.

The CMS begins listening on the port number you specified. The Server Intelligence Agent dynamically propagates the new settings to the other servers on the node, if those servers have the Auto-Assign option selected for the request port. (It may take several minutes for your changes to appear in the Properties settings of all node members.) If no CMS is running on the cluster, you must use the CCM to change the port number.

To change the default CMS port in the CCM

If no CMS is running on the cluster, you must use the CCM to change the CMS port number.

1. Open the CCM and stop the SIA for the node.
2. Right-click the SIA and choose **Properties**.
3. In the "Properties" dialog box, click the "Startup" tab.
4. From the "Local CMS Servers" list select the CMS and click **Properties**.
5. To bind the CMS to a specific port, type in the **Port** field one of the following:
 - port number
 - the hostname of the target NIC and port number (use the hostname:port number format)
 - the IP address of the target NIC and port number (use the IP address:port number format)
6. Click **OK** to apply the new settings.
7. Start the SIA and wait for the servers to start.

To change the port a CMS uses for accepting requests

1. Go to the "Servers" management area of the CMC.
2. Select the CMS, then choose **Properties** from the **Manage** menu.
3. Under **Common Settings**, deselect the **Auto-Assign** check box for **Request Port**, then type the port number you want the server to listen on.
4. Click **Save** or **Save & Close**.
5. Restart the CMS.

The CMS binds to the new port, and starts listening for requests from other servers.

To change the port a server uses for accepting requests

Note:

These steps cannot be used to change the request port for the Central Management Server (CMS). See “To change the port a CMS uses for accepting requests” instead.

1. Go to the "Servers" management area of the CMC.
2. Select the server, then choose **Stop Server** from the **Actions** menu.
3. Choose **Properties** from the **Manage** menu.
4. Under **Common Settings**, deselect the **Auto-Assign** check box for **Request Port**, then type the port number you want the server to listen on.
5. Click **Save** or **Save & Close**.
6. Start and enable the server.

The server binds to the new port, registers with the CMS, and begins listening for BusinessObjects Enterprise requests on the new port.

Changing the connect port used by Tomcat

During the installation, the default port used for Tomcat is 8080. If this port is already in use by another instance of Tomcat, or if another application is using this port, you will need to change the connect port used by Tomcat.

To change the Tomcat connect port

1. Stop Tomcat server by selecting the server name and clicking on the stop button.
2. Open the server.xml file for Tomcat in a text editor.

On Windows, this file can normally be found in the following directory:

C:\Program Files\Business Objects\Tomcat\conf

3. Locate the following string:

```
<Connector URIEncoding="UTF-8" acceptCount="100" connectionTimeout="20000" debug="0" disableUploadTimeout="true" enableLookups="false" maxSpareThreads="75"
```

```
maxThreads="150" minSpareThreads="25" port="8080"  
redirectPort="8443" />
```

4. Change port 8080 to an available port number.
5. Save and close the file.

Managing CMS system database connections

If the CMS system database is unavailable, for example due to a hardware or software failure or a network problem, the CMS goes into the “Waiting for resources” state. If the system database is on a BusinessObjects Enterprise deployment that has multiple CMSs, then subsequent requests are forwarded to any CMSs in the cluster that have an active connection to the system database. While a CMS is in the “Waiting for resources” state, any current requests that do not require database access continue to be processed, but requests that require access to the CMS database will fail.

By default, a CMS in the “Waiting for resources” state periodically attempts to reestablish the number of connections that are specified in the “System Database Connections Requested” property. As soon as the database connections are established, goes into the “Running” state, and resumes normal operations.

In some cases, you may want to prevent the CMS from automatically reestablishing a connection to the database. For example, you may want to verify the integrity of the database before database connections are reestablished. To do so, on the "Properties" page of the CMS server, check **Disable Auto Reconnect to System and Auditing Databases**.

Related Topics

- [To change a server's properties](#)

Copying data from one CMS system database to another

BusinessObjects Enterprise enables you to copy the contents of one CMS system database into another database. You can copy CMS data from a different CMS database (versions 8.5 through 10 of Crystal Enterprise and

version XI and XI R2 of BusinessObjects Enterprise) into your current CMS system database. Or, you can copy the data from your current CMS system database into a different data source.

Throughout this section, the “source” CMS database refers to the database that holds the data you are copying; this data is copied into the “destination” (or “target”) database. The destination database is initialized before the new data is copied in, so any existing contents of the destination database are permanently deleted (all BusinessObjects Enterprise tables are destroyed permanently and then recreated). Once the data has been copied, the destination database is established as the current database for the CMS.

Tip:

If you want to import users, groups, folders, and reports from one system to another, without deleting the contents of the current CMS database, use the Import Wizard. For more information, click Help in the Import Wizard.

Depending on the platform of your system and the version of your CMS database, copying a CMS database may include the following tasks:

- [Preparing to copy a CMS system database](#)
- [Changing the name of a CMS cluster](#)

When you finish copying data from the source database to the destination database, complete these steps before allowing users to access the system.

Server groups from the old installation appear in the new system, but they will be empty. New servers are automatically detected and added to the servers list (outside of any group) in a disabled state. You must enable these servers before they can be used. You may add the new servers to the imported groups as appropriate.

Reports that depend on a particular server group for scheduled processing will not execute until a job server is added to that group. Reports that depend on a particular server group for processing are not available until servers are added to that group.

Note:

When upgrading from an older version of Crystal Enterprise, servers that existed in the source installation do not appear in the upgraded install. This occurs because there cannot be a mix of old and new servers in a BusinessObjects Enterprise installation.

Note:

If errors occurred during an upgrade, a `db_migration` log file was created in the logging directory on the machine where you performed the migration. You will be prompted if you need to check the log file. The default logging directory is: `C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Logging\` on Windows and `BusinessObjects_root/logging` on UNIX (where `BusinessObjects_root` is the absolute path to the root Business Objects directory of your BusinessObjects Enterprise installation).

To copy a CMS system database on Windows

Note:

If you are copying a CMS database from an R3 source destination to an R3 target destination, you can change the CMS location, name, and database type. However, you cannot change the BusinessObjects Enterprise installation path, operating system, and machine name.

1. Open the Central Configuration Manager (CCM) and stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and choose **Properties**.
3. Click the **Configuration** tab, and then click **Specify**.
4. Choose **Copy**, then click **OK**.
5. Choose the version information for the source CMS database.
6. Select the database type for the source CMS database, and then specify its database information (including host name, user name, and password).
7. Select the database type for the destination CMS database, and then specify its database information (including host name, user name, and password).
8. When the CMS database has finished copying, click **OK**.
9. If you are upgrading from an earlier version than R3, you will be prompted to build a Server Intelligence Agent.
 - a. Click **OK**.
 - b. Specify the administrator password, and then click **OK**.
 - c. When the SIA is built, click **OK**.
10. Proceed to [To change the directories of the Input and Output File Repository Servers on Windows](#).

To copy a CMS system database on Unix

Note:

If you are copying a CMS database from an R3 source destination to an R3 target destination, you can change the CMS location, name, and database type. However, you cannot change the BusinessObjects Enterprise installation path, operating system, and machine name.

1. Run `cmsdbsetup.sh` (located in `<InstallDirectory>/bobje/`, by default).
2. Select the "copy" option (option 4), then confirm your choice.
3. Select the version information for the source CMS database.
4. Select the database type for the source CMS database, then specify its database information (including host name, user name, and password).
5. Select the database type for the destination CMS database, and then specify its database information (including host name, user name, and password).

The CMS database is copied to the destination machine. A message appears when the copy is complete.

6. If you are upgrading from an earlier version than R3, you will be prompted to build a Server Intelligence Agent. Specify the administrator password. A message appears when the SIA is built.
7. Proceed to [To change the directories of the Input and Output File Repository Servers on Unix](#).

Changing the directories of the Input and Output File Repository Servers

In order to upgrade your objects after you copy a CMS system database to a new CMS database, you need to point your Input and Output File Repository servers to new source directories. The following procedures show how to do this on Windows and on Unix.

To change the directories of the Input and Output File Repository Servers on Windows

1. If you copied CMS data from a different CMS system database into your current CMS database, you need to make your old input and output

directories available to the new Input and Output File Repository Servers. You can do this in several ways:

- Copy the contents of the original input root directory into the root directory that the new Input File Repository Server is already configured to use. Then copy the contents of the original output directory into the root directory that the new Output File Repository is already configured to use.
- Reconfigure the new Input and Output File Repository Servers to use the old input and output root directories.
- If the old Input and Output File Repository Servers are running on a dedicated machine, you can run the BusinessObjects Enterprise setup program to upgrade the servers directly. Then you need not move the input and output directories.

2. Use the CCM to start the SIA on the local machine.
3. Make sure your web application server is running.
4. Log on to the CMC with the default Administrator account, using Enterprise authentication.

Tip:

If you just replaced your CMS system database with data from an older system, keep in mind that you now need to provide the Administrator password that was valid in the older system.

5. In the CMC, go to the **License Keys** management area and check that your BusinessObjects Enterprise license keys are entered correctly.
6. Go to the **Servers** management area of the CMC and start and enable the Input File Repository Server and the Output File Repository Server.
7. For each File Repository Server, choose **Properties** on the **Manage** menu, then check that the **File Store Directory** points to the correct location.
8. If objects in your source database require updating, click **Update Objects**.
9. When prompted, log on to your CMS with credentials that provide you with administrative privileges to BusinessObjects Enterprise.

The Update Objects dialog box tells you how many objects require updating. Objects typically require updating because their internal representation has changed in the new version of BusinessObjects Enterprise, or because the objects require new properties to support the additional features offered by BusinessObjects Enterprise. Because your

Central Management Server was stopped when the data was copied, you need to update the objects now.

10. If there are objects that require updating, click **Update**, otherwise click **Cancel**.

Note:

LDAP and Windows AD authentication will not be available until after the Update Objects task has been completed.

11. Start and enable the remaining BusinessObjects Enterprise servers.

Verify that BusinessObjects Enterprise requests are handled correctly, and check that you can view and schedule reports successfully.

To change the directories of the Input and Output File Repository Servers on Unix

1. If you copied CMS data from a different CMS system database into your current CMS database, you need to make your old input and output directories available to the new Input and Output File Repository Servers. You can do this in several ways:
 - Copy the contents of the original input root directory into the root directory that the new Input File Repository Server is already configured to use. Then copy the contents of the original output directory into the root directory that the new Output File Repository is already configured to use.
 - Reconfigure the new Input and Output File Repository Servers to use the old input and output root directories.
 - If the old Input and Output File Repository Servers are running on a dedicated machine, you can run the BusinessObjects Enterprise setup program to upgrade the servers directly. Then you need not move the input and output directories. For more information, see [Setting root directories and idle times of the File Repository Servers](#).
2. Make sure your web application server is running.
3. Log on to the Central Management Console with the default Administrator account, using Enterprise authentication.

Tip:

If you just replaced your CMS database with data from an older system, keep in mind that you now need to provide the Administrator password that was valid in the older system.

4. Use the Central Management Console (CMC) to start the CMS on the local machine.
5. Go to the **License Keys** management area and check that your BusinessObjects Enterprise license keys are entered correctly.
6. Go to the **Servers** management area of the CMC and start and enable the Input File Repository Server and the Output File Repository Server.
7. Click the link to each File Repository Server and, on the **Properties** tab, check that the **File Store Directory** points to the correct location.
8. Run the `ccm.sh` script. If you migrated a source database from an earlier version of BusinessObjects Enterprise, enter the following command:

```
./ccm.sh -updateobjects authentication info
```

See the UNIX Tools chapter of the *SAP BusinessObjects Enterprise Administrator's Guide* for information on the authentication information required by `ccm.sh`.

Objects typically require updating because their internal representation has changed in the new version of BusinessObjects Enterprise, or because the objects require new properties to support the additional features offered by BusinessObjects Enterprise XI.

9. Use the CMC to start and enable the remaining BusinessObjects Enterprise servers.
10. Verify that BusinessObjects Enterprise requests are handled correctly, and check that you can view and schedule reports successfully.

Preparing to copy a CMS system database

Before copying a CMS system database, take the source and the destination environments offline by disabling and subsequently stopping all servers. Back up both CMS databases, and back up the root directories used by all Input and Output File Repository Servers. If necessary, contact your database or network administrator.

Ensure that you have a database user account that has permission to read all data in the source database, and a database user account that has Create, Delete, and Update rights to the destination database. Also ensure also that you can connect to both databases—through your database client software

or through ODBC, according to your configuration—from the CMS machine whose database you are replacing.

If you are copying the CMS database as part of an upgrade installation, make a note of the license keys you purchased for the current version of BusinessObjects Enterprise. License keys that are present in the destination database are retained only if the source database contains no license keys that are valid for the current version of BusinessObjects Enterprise. License keys in the destination database are replaced with license keys from the source database when the source license keys are valid for the current version of BusinessObjects Enterprise. License keys from earlier versions of Crystal Enterprise are not copied.

If you are copying CMS data from a different CMS database (version 8.5, 9, or 10 of Crystal Enterprise or version XI or XI R2 of BusinessObjects Enterprise) into your current CMS database, your current CMS database is the destination database whose tables are deleted before they are replaced with the copied data. In this scenario, make note of the current root directories used by the Input and Output File Repository Servers in the source environment. Report files are not moved from one directory location to another. After you copy the database, you will connect your new Input and Output File Repository Servers to the old root directories, thus making the report files available for the new system to process. Log on with an administrative account to the CMS machine whose database you want to replace. Complete the procedure that corresponds to the version of the source environment:

- *Copying data from one CMS system database to another*

If you are copying a CMS database from its current location to a different database server, your current CMS database is the source environment. Its contents are copied to the destination database, which is then established as the active database for the current CMS. This is the procedure to follow if you want to move the default CMS database on Windows from the local Microsoft Data Engine (MSDE) to a dedicated database server, such as Microsoft SQL Server, Informix, Oracle, DB2, or Sybase. Log on with an administrative account to the machine that is running the CMS whose database you want to move. Complete the following procedure:

- *Copying data from one CMS system database to another*

Note:

- When you upgrade a CMS database from an earlier version, the database and database schema are upgraded to the format required by the current version of BusinessObjects Enterprise.
- When you copy data from one database to another, the destination database is initialized before the new data is copied in. That is, if your destination database does not contain the four BusinessObjects Enterprise XI system tables, these tables are created. If the destination database does contain BusinessObjects Enterprise XI system tables, the tables will be permanently deleted, new system tables will be created, and data from the source database will be copied into the new tables. Other tables in the database, including previous versions of Crystal Enterprise system tables, are unaffected.

Deleting and recreating the CMS system database

This procedure shows how to recreate (re-initialize) the current CMS system database. By performing this task, you destroy all data that is already present in the database. This procedure is useful, for instance, if you have installed BusinessObjects Enterprise in a development environment for designing and testing your own, custom web applications. You can re-initialize the CMS system database in your development environment every time you need to clear the system of all its data.

Caution:

By implementing the steps outlined in this workflow, you will delete of all data in the CMS database as well as objects such as reports and users. Do not perform these steps on a production deployment.

In this version of BusinessObjects Enterprise, server configuration information is stored in the CMS system database. It is very important that you back up all server configuration files before re-initializing the CMS system database. When you recreate the database, your server configuration information will be erased and you must have a backup in order to restore this information.

When you recreate the system database, your existing license keys should be retained in the database. However, if you need to enter license keys again, log on to the CMC with the default Administrator account (which will have been reset to have no password). Go to the Authorization management area and enter your information on the License Keys tab.

Note:

If you re-initialize your CMS system database, all data in your current CMS system database will be destroyed. Consider backing up your current database before beginning. If necessary, contact your database administrator.

To recreate the CMS system database on Windows

1. Use the CCM to stop the Server Intelligence Agent (SIA).

Note:

For this procedure, you cannot run the CCM on a remote machine; it must be run on a machine with at least one valid node.

2. Right-click the SIA and choose **Properties**.
3. In the **Properties** dialog box, in the CMS Data Source area, click **Specify**.
4. In the **CMS Database Setup** dialog box, click **Recreate the current Data Source**.

Note:

All servers and objects from the machine where you ran the CCM in step 1 will also be recreated.

5. Click **OK** and, when prompted to confirm, click **Yes**.

The CCM notifies you when the CMS system database setup is complete.

6. Click **OK**.

You are returned to the CCM.

7. Restart the Server Intelligence Agent and enable services.

While it is starting, the Server Intelligence Agent starts the CMS. The CMS writes required system data to the newly emptied data source.

8. If prompted, click **Update Objects**.
9. If your deployment has more than one machine, you need to re-create the nodes on the other machines.

Note:

When you recreate the CMS system database, the information stored on the other machines continues to refer to the original database. The nodes must be recreated so this information is updated to the recreated CMS system database. For more information, see [Working with nodes](#).

To recreate the CMS system database on UNIX

Use the `cmsdbsetup.sh` script. For reference, see the UNIX Tools chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

1. Run `cmsdbsetup.sh` (located in `<InstallDirectory>/bobje/`, by default).
2. Select the "reinitialize" option (option 5), then confirm your choice.
The `cmsdbsetup.sh` script begins recreating the CMS system database.
3. Provide your administrator password and the CMS port number you want.
4. When the database creation is complete, exit the `cmsdbsetup.sh` script.
5. Provide the database information (for example: host name, user name, and password).

A notification message appears when the CMS database has been pointed to the new location.

6. If you are prompted to rebuild the Server Intelligence Agent (SIA), provide the administrator password and the port number you want to CMS to communicate on.

Note:

You will be prompted for this information only if you point to an empty CMS database.

7. Use the following command to run the `ccm.sh` script (located in `<InstallDirectory>/bobje/`, by default):

```
ccm.sh -start SIANAME
```

8. To enable the services, use the following command:

```
ccm.sh -enable all -cms CMSNAME:PORT -username administrator -password password
```

Note:

Since you just recreated the CMS database, the administrator password is blank.

9. To update the objects, use the following command:

```
ccm.sh -updateobjects -cms CMSNAME:PORT -username administrator -password password
```

Selecting a new or existing CMS database

You can use the CCM to specify a new or existing CMS system database for a node. Generally, there are only a few times when you need to complete these steps:

- If you have changed the password for the current CMS system database, these steps allow you to disconnect from, and then reconnect to, the current database. When prompted, you can provide the CMS with the new password.
- If you want to select and initialize an empty database for BusinessObjects Enterprise, these steps allow you to select that new data source.
- If you have restored a CMS system database from backup (using your standard database administration tools and procedures) in a way that renders the original database connection invalid, you will need to reconnect the CMS to the restored database. (This might occur, for instance, if you restored the original CMS database to a newly installed database server.)

Note:

In earlier versions of BusinessObjects Enterprise, this procedure was used to add a CMS to a cluster. Do not use this procedure to add a CMS to a cluster. Clustering is now handled by nodes. For information on moving servers between clusters, see [Backing up and restoring server configuration settings](#).

To select a new or existing CMS database on Windows

Note:

This procedure is not used for clustering CMS services. For information on moving servers between clusters, see [Backing up and restoring server configuration settings](#).

Note:

When you select a new or existing CMS database on Windows, the BusinessObjects installation path, operating system, and machine name cannot change.

1. Use the CCM to stop the Server Intelligence Agent (SIA).
2. Select the SIA and click **Specify CMS System Database Data Source** on the toolbar.
3. In the **Configuration** tab of the "Properties" dialog box, under **CMS Data Source**, click **Specify**.
4. The remaining steps depend upon the connection type you selected:
 - If you selected ODBC, the Windows "Select Data Source" dialog box appears. Select the ODBC data source that you want to use as the CMS database; then click OK. (Click New to configure a new DSN.) When prompted, provide your database credentials and click OK.
 - If you selected a native driver, you are prompted for your database Server Name, your Login ID, and your Password. Provide this information and then click OK.

The CCM notifies you when the CMS database setup is complete.

5. In the "Properties" dialog box, click **OK**.
6. Restart the Server Intelligence Agent.

To select a new or existing CMS database on UNIX

Use the `cmsdbsetup.sh` script. For reference, see the UNIX Tools chapter.

1. Run the `cmsdbsetup.sh` script (located by default in `<InstallDirectory>/bobje/`).
2. Select the update action (option 6).
3. When prompted, provide the database type of the new CMS database.
4. Provide the database information (for example: host name, user name, and password).

A notification message appears when the CMS database has been pointed to the new location.

5. If you are prompted to rebuild the Server Intelligence Agent (SIA), provide the administrator password and the port number you want to CMS to communicate on.

Note:

You will be prompted for this information only if you point to an empty CMS database.

Setting root directories and idle times of the File Repository Servers

The Properties tabs of the Input and Output File Repository Servers enable you to change the locations of the default root directories. These root directories contain all of the report objects and instances on the system. You may change these settings if you want to use different directories after installing BusinessObjects Enterprise, or if you upgrade to a different drive (thus rendering the old directory paths invalid).

Note:

- The Input and Output File Repository Servers must not share the same root directory, because modifications to the files and subdirectories belonging to one server could have adverse effects on the other server. In other words, if the Input and Output File Repository Servers share the same root directory, then one server might damage files belonging to the other.
- If you run multiple File Repository Servers, all Input File Repository Servers must share the same root directory, and all Output File Repository Servers must share the same root directory (otherwise there is a risk of having inconsistent instances).
- It is recommended that you replicate the root directories using a RAID array or an alternative hardware solution.
- The root directory should be on a drive that is local to the server.

You can also set the maximum idle time of each File Repository Server. This setting limits the length of time that the server waits before it closes inactive connections. Before you change this setting, it is important to understand that setting a value too low can cause a user's request to be closed prematurely. Setting a value too high can cause excessive consumption of system resources such as processing time and disk space.

To modify settings for a File Repository Server

1. Go to the "Servers" management area of the CMC.
2. Select the File Repository Server you want to change.
3. Choose **Properties** from the **Manage** menu.
4. In the "Properties" dialog box, make your changes and then click **Save** or **Save & Close**.

Modifying performance settings

You can change performance settings for BusinessObjects Enterprise servers. For information about assessing your system's performance and using these configuration settings, see the Improving Performance chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

Configuring destinations for job servers

By default, when the system runs a scheduled report or a program object, it stores the output instance it creates on the Output File Repository Server (FRS). However, you can specify a different destination. If you do, the system will store one output instance on the Output FRS, and one at the specified destination.

You also specify a destination when you use the Send to feature, which sends an existing object to a specified destination.

In order for the system to work with destinations other than the default, the destination you are sending to must be enabled and configured on all Destination Job Servers in the system.

For example, to be able to schedule a report object for output to an unmanaged disk, you have to enable and configure the Unmanaged Disk destination on the Destination Job Server in the system. To send a report instance by email, you have to configure the Email (SMTP) destination on the Destination Job Servers.

Configuring destinations for job servers includes:

- [To enable or disable destinations for a job server](#)

- [Configuring the destination properties for job servers](#)

For information about selecting destinations for objects see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To enable or disable destinations for a job server

For a 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. See also [Configuring the destination properties for job servers](#).

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 BusinessObjects Enterprise system. If you want, you can enable and configure additional destinations on the Destination Job 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**.

Note:

If you enabled the destination, you must also configure the destination. See [Configuring the destination properties for job servers](#).

6. To disable a destination, select it in the **Destination** list and click **Remove**.
7. Click **Save** or **Save & Close**.

Configuring the destination properties for job servers

This procedure applies to the following servers:

- Program Job Server
- Report Job Server
- Destination Job Server
- Desktop Intelligence Job Server

For a job server to store output instances in a destination other than the default, you have to enable and configure the other destinations on the appropriate job servers. See also [Configuring destinations for job servers](#).

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. For information about the properties for each destination, see:
 - [Inbox destination properties](#)
 - [File System destination properties](#)
 - [FTP destination properties](#)
 - [Email destination properties](#)
7. Click **Save** or **Save & Close**.
8. Make sure the destination has been enabled. See [To enable or disable destinations for a job server](#).

Inbox destination properties

The Inbox destination stores an object or instance in the user inboxes on the BusinessObjects Enterprise system. A user inbox is automatically created when you add a user. For more information, see [Configuring the destination properties for job servers](#) and "Setting rights" in the *SAP BusinessObjects Enterprise Administrator's Guide*.

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 BusinessObjects Enterprise system. If you want, you can enable and configure additional destinations on the Destination 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.

Email destination properties

The following settings are available for email destinations. See also [Configuring the destination properties for job servers](#).

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 BusinessObjects Enterprise 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.

FTP destination properties

The following settings are available for FTP destinations. See also [Configuring the destination properties for job servers](#).

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 BusinessObjects Enterprise 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.

File System destination properties

A file system destination is an unmanaged disk destination on a system outside the BusinessObjects Enterprise system. See also [Configuring the destination properties for job servers](#).

Directory

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

Automatically Generated

Select this option if you want BusinessObjects Enterprise 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 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 Job Server permission to write files to the remote directory.

Configuring Windows processing servers for your data source

When started on Windows, the report processing servers by default log on to the local system as services with the Windows "LocalSystem" account. This account determines the permissions that each service is granted on the local machine. This account does not grant the service any network permissions.

In the majority of cases, this account is irrelevant in relation to the server's task of processing reports against your data source. (The database logon credentials are stored with the report object.) Thus, you can usually leave each server's default logon account unchanged or, if you prefer, you can change it to a Windows user account with the appropriate permissions.

However, there are certain cases when you must change the logon account used by the processing servers. These cases arise either because the server needs additional network permissions to access the database, or because the database client software is configured for a particular Windows user account. This table lists the various database/ driver combinations and shows when you must complete additional configuration.

Tip:

Running a service under an Administrator account does not inadvertently grant administrative privileges to another user, because users cannot impersonate services.

Related Topics

- [Changing the system user account](#)

Configuring UNIX processing servers for your data source

The Job Servers and Processing Servers support native and ODBC connections to a number of reporting databases. This section discusses the environment variables, software, and configuration files that must be available to the servers in order for them to process reports successfully. Whether your reports use native or ODBC drivers, ensure that the reporting environment configured on the server accurately reflects the reporting environment configured on the Windows machine that you use when designing reports.

Related Topics

- [Native drivers](#)
- [ODBC drivers](#)

Native drivers

If you design reports using native drivers, you must install the appropriate database client software on each Job Server and/or Processing Server machine that will process the reports. The server loads the client software at runtime in order to access the database that is specified in the report. The server locates the client software by searching the library path environment variable that corresponds to your operating system (`LD_LIBRARY_PATH` on Sun Solaris, `LIBPATH` on IBM AIX, and so on), so this variable must be defined for the login environment of each Job Server and Processing Server.

Depending on your database, additional environment variables may be required for the Job Server and Processing Server to use the client software. These include:

- **Oracle**

The `ORACLE_HOME` environment variable must define the top-level directory of the Oracle client installation.

- **Sybase**

The SYBASE environment variable must define the top-level directory of the Sybase client installation. The SYBPLATFORM environment variable must define the platform architecture.

- **DB2**

The DB2INSTANCE environment variable must define the DB2 instance that is used for database access. Use the DB2 instance initialization script to ensure that the DB2 environment is correct.

Note:

For complete details regarding these and other required environment variables, see the documentation included with your database client software.

As an example, suppose that you are running reports against both Sybase and Oracle. The Sybase database client is installed in `/opt/sybase`, and the Oracle client is installed in `/opt/oracle/app/oracle/product/8.1.7`. You installed BusinessObjects Enterprise under the `crystal` user account (as recommended in the *SAP BusinessObjects Enterprise Installation Guide*).

If the `crystal` user's default shell is a C shell, add these commands to the `crystal` user's login script:

```
setenv LD_LIBRARY_PATH /opt/oracle/app/oracle/product/8.1.7/lib:opt/sybase/lib:$LD_LIBRARY_PATH
setenv ORACLE_HOME /opt/oracle/app/oracle/product/8.1.7
setenv SYBASE /opt/sybase
setenv SYBPLATFORM sun_svr4
```

If the `crystal` user's default shell is a Bourne shell, modify the syntax accordingly:

```
LD_LIBRARY_PATH=/opt/oracle/app/oracle/product/8.1.7/lib:opt/sybase/lib:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH
ORACLE_HOME=/opt/oracle/app/oracle/product/8.1.7;export ORACLE_HOME
SYBASE=/opt/sybase;export SYBASE
SYBPLATFORM=sun_svr4;export SYBPLATFORM
```

ODBC drivers

If you design reports off ODBC data sources (on Windows), you must set up the corresponding data sources on the Job Server and Processing Server machines. In addition, you must ensure that each server is set up properly for ODBC. During the installation, BusinessObjects Enterprise installs ODBC drivers for UNIX, creates configuration files and templates related to ODBC reporting, and sets up the required ODBC environment variables. This section discusses the installed environment, along with the information that you need to edit.

Note:

- If you report off DB2 using ODBC, your database administrator must first bind the UNIX version of the driver to every database that you report against (and not just each database server). The bind packages are installed below the `crystal/enterprise/platform/odbc/lib` directory; their filenames are `iscsso.bnd`, `iscswwho.bnd`, `isrrso.bnd`, `isrrwho.bnd`, `isurso.bnd`, and `isurwho.bnd`. Because Crystal Reports runs on Windows, ensure that the Windows version of the driver has been bound to each database.
- On UNIX, BusinessObjects Enterprise does not include the Informix client-dependent ODBC driver (CRinf16) that is installed on Windows. The UNIX version does, however, include the clientless ODBC driver for Informix connectivity.

ODBC environment variables

The environment variables related to ODBC reporting are: the library path that corresponds to your operating system (`LD_LIBRARY_PATH` on Sun Solaris, `LIBPATH` on IBM AIX, and so on), `ODBC_HOME`, and `ODBCINI`. The BusinessObjects Enterprise installation includes a file called `env.csh` that is sourced automatically every time you start the BusinessObjects Enterprise servers with the CCM. Thus, the environment for the Job Server and Processing Server is set up automatically:

- The `INSTALL_ROOT/bobje/enterprise120/platform/odbc/lib` directory of your installation is added to the library path environment variable.
- The `ODBC_HOME` environment variable is set to the `INSTALL_ROOT/bobje/enterprise120/platform/odbc` directory of your installation.

- The `ODBCINI` environment variable is defined as the path to the `.odbc.ini` file that was created by the BusinessObjects Enterprise installation.

Modify the environment variables in the `env.csh` script only if you have customized your configuration of ODBC. The main ODBC configuration file that you need to modify is the system information file.

Working with the ODBC system information file

The system information file (`odbc.ini`) is created in the `HOME` directory of the user account under which you installed BusinessObjects Enterprise (typically the `crystal` user account). In this file, you define each of the ODBC data sources (DSNs) that the Job Server and Processing Server need in order to process your reports. The BusinessObjects Enterprise installation completes most of the required information—such as the location of the ODBC directory and the name and location of each installed ODBC driver—and shows where you need to provide additional information.

Tip:

A template of the system information file is installed to `INSTALL_ROOT/bobje/defaultodbc.ini`

The following example shows the contents of a system information file that defines a single ODBC DSN for servers running on UNIX. This DSN allows the Job Server and Processing Server to process reports based on a System DSN (on Windows) called `CRDB2`:

```
[ODBC Data Sources]
CRDB2=MERANT 3.70 DB2 ODBC Driver

[CRDB2]
Driver=/opt/bobje/enterprise120/platform/odbc/lib/crdb216.so
Description=MERANT 3.70 DB2 ODBC Driver
Database=myDB2server
LogonID=username
[ODBC]
Trace=0
TraceFile=odbctrace.out
TraceDll=/opt/bobje/enterprise120/platform/odbc/lib/odbc
trac.so
InstallDir=/opt/bobje/enterprise120/platform/odbc
```

As shown in the example above, the system information file is structured in three major sections:

- The first section, denoted by `[ODBC Data Sources]`, lists all the DSNs that are defined later in the file. Each entry in this section is provided as `dsn=driver`, and there must be one entry for every DSN that is defined in the file. The value of `dsn` must correspond exactly to the name of the System DSN (on Windows) that the report was based off.
- The second section sequentially defines each DSN that is listed in the first section. The beginning of each definition is denoted by `[dsn]`. In the example above, `[CRDB2]` marks the beginning of the single DSN that is defined in the file.

Each DSN is defined through a number of option=value pairs. The options that you must define depend upon the ODBC driver that you are using. These pairs essentially correspond to the Name=Data pairs that Windows stores for each System DSN in the registry:

```
\\HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\odbc.ini\dsn
```

However, the options for a particular ODBC driver on UNIX may not correspond by name to the options available for a Windows version of the same driver. For example, some Windows drivers store a UID value in the registry, and on UNIX you may need to specify this value with the LogonID option.

The final section of the file, denoted by `[ODBC]`, includes ODBC tracing information. You need not modify this section.

When the installation creates the system information file, it completes some fields and sets up a number of default DSNs—one for each of the installed ODBC drivers. The standard options that are commonly required for each driver are included in the file (`Database=`, `LogonID=`, and so on). Edit the file and provide the corresponding values that are specific to your reporting environment.

This example shows the entire contents of a system information file created when BusinessObjects Enterprise was installed to the `/usr/local` directory.

```
[ODBC Data Sources]
CRDB2=MERANT 3.70 DB2 ODBC Driver
CRINF_CL=MERANT 3.70 Informix Dynamic Server ODBC Driver
CROR8=MERANT 3.70 Oracle8 ODBC Driver
CRSS=MERANT 3.70 SQL Server ODBC Driver
```



```

CRSYB=MERANT 3.70 Sybase ASE ODBC Driver
CRTXT=MERANT 3.70 Text ODBC Driver

[CRDB2]
Driver=/usr/local/bobje/enterprise120/plat
form/odbc/lib/crdb216.so
Description=MERANT 3.70 DB2 ODBC Driver
Database=
LogonID=

[CRINF_CL]
Driver=/usr/local/bobje/enterprise120/plat
form/odbc/lib/crifcl16.so
Description=MERANT 3.70 Informix Dynamic Server ODBC
Driver
ServerName=
HostName=
PortNumber=
Database=
LogonID=

[CROR8]
Driver=/usr/local/bobje/enterprise120/plat
form/odbc/lib/cror816.so
Description=MERANT 3.70 Oracle8 ODBC Driver
ServerName=
ProcedureRetResults=1
LogonID=

[CRSS]
Driver=/usr/local/bobje/enterprise120/plat
form/odbc/lib/crmsss16.so
Description=MERANT 3.70 SQL Server ODBC Driver
Address=
Database=
QuotedId=Yes
LogonID=

[CRSYB]
Driver=/usr/local/bobje/enterprise120/plat
form/odbc/lib/crase16.so
Description=MERANT 3.70 Sybase ASE ODBC Driver
NetworkAddress=
Database=
LogonID=

[CRTXT]
Driver=/usr/local/bobje/enterprise120/plat

```

```
form/odbc/lib/crtxt16.so
Description=MERANT 3.70 Text ODBC Driver
Database=

[ODBC]
Trace=0
TraceFile=odbctrace.out
TraceDll=/usr/local/bobje/enterprise120/platform/odbc/
form/odbc/lib/odbcdrac.so
InstallDir=/usr/local/bobje/enterprise120/platform/odbc
```

Adding a DSN to the default ODBC system information file

When you need to add a new DSN to the installed system information file (`.odbc.ini`), first add the new DSN to the bottom of the `[ODBC Data Sources]` list. Then add the corresponding `[dsn]` definition just before the `[ODBC]` section.

For example, suppose that you have a Crystal report that uses ODBC drivers to report off your Oracle8 database. The report is based off a System DSN (on Windows) called SalesDB. To create the corresponding DSN, first append this line to the `[ODBC Data Sources]` section of the system information file:

```
SalesDB=MERANT 3.70 Oracle8 ODBC Driver
```

Then define the new DSN by adding the following lines just before the system information file's `[ODBC]` section:

```
[SalesDB]
Driver=/usr/local/bobje/enterprise120/platform/odbc/lib/cror816.so
Description=MERANT 3.70 Oracle8 ODBC Driver
ServerName=MyServer
ProcedureRetResults=1
LogonID=MyUserName
```

Once you have added this information, the new DSN is available to the Job Server and Processing Server, so they can process reports that are based off the SalesDB System DSN (on Windows).

Adding and removing Windows server dependencies

When installed on Windows, each Server Intelligence Agent (SIA) in BusinessObjects Enterprise is dependent on the Event Log and Remote Procedure Call (RPC) services. If you are having problems with an SIA, check to ensure that all three services appear on the SIA's Dependency tab.

To add and remove server dependencies

1. Use the CCM to stop the Server Intelligence Agent (SIA) whose dependencies you want to modify.
2. Right-click the SIA and choose **Properties**.
3. Click the **Dependency** tab.
4. To add a dependency to the list, click **Add**.

The Add Dependency dialog box provides you with a list of all available dependencies. Select the dependency or dependencies, as required, and then click **Add**.

5. To remove a dependency from the list, select it and click **Remove**.
6. Click **OK**.
7. Restart the SIA.

Changing the system user account

If the incorrect user account is running the Server Intelligence Agent, you can change it in the Central Configuration Manager (CCM). Note that all servers managed by a Server Intelligence Agent run under the same account.

Note:

If you want to run a Program Job Server on a Windows machine under any account other than the system account, you must ensure that:

- The account is a member of the Local Administrator's group on the machine that the Program Job Server is running.
- The account must have the "Replace process level token" right granted to it under "Local Security Settings".

To change an SIA's user account

1. Use the CCM to stop the Server Intelligence Agent.
2. Right-click the Server Intelligence Agent and choose **Properties**.
3. Clear the **System Account** check box.
4. Enter the user name and password information.

When started, the server process will log on to the local machine with this user account. In addition, all objects processed by this server will be formatted using the printer settings associated with the user account that you enter.

Note:

All servers managed by a Server Intelligence Agent run under the same account.

5. Click **OK**.
6. Restart the Server Intelligence Agent.

Configuring tracing for servers

Every BusinessObjects Enterprise server or process has its own log trace files. The trace log file name is composed of the process (server) name, process ID, and full date. For example, AAAnalyt
ics_2344_2008_09_10_21_24_666_trace.log. The _trace.log files are by default stored in the following directories :

- On Windows: <INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\logging
- On UNIX: <INSTALLDIR>/boobje/logging

To help administrators identify and resolve problems with BusinessObjects Enterprise servers, all errors and critical events (asserts) are by default traced and written to a log file. In addition to errors and asserts, servers can be traced for warning and success messages.

You can modify the tracing severity threshold or any other tracing-related settings through either of the following:

- BO_trace.ini file

- Server command line through the CMC

To configure server tracing through the BO_trace.ini file

The BO_trace.ini file is read every minute and by default it is configured to disable tracing. To activate and configure tracing using the BO_trace.ini file, please follow these steps:

1. Go to the "Servers" management area of the CMC.
2. Select the server, then choose **Stop Server** from the **Actions** menu.
3. Choose **Properties** from the **Manage** menu.
4. To specify the default location for the BO_trace.ini, enter the following under "Command Line Parameters":

```
-configFile <$INSTALLDIR\BusinessObjects Enterprise
12.0\logging\logConfig\BO_trace.ini>
```

5. Click **Save & Close**.
6. Restart the server.
7. Open the BO_trace.ini file.
 - The default location on Windows is:


```
<INSTALLDIR>\BusinessObjects Enterprise
12.0\logging\logConfig.
```
 - The default location on UNIX is: <INSTALLDIR>/boobje/log
 ging/LogConfig.
8. Uncomment the required lines under the "Trace Syntax and Setting" section.
9. Modify the server tracing parameters as required.

The table below lists all the available parameters for configuring server tracing.

Parameter	Possible values	Description
active	false, true	Enables tracing for the current process or server if set to true. Default value is false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl Note: importance = xs is the most verbose option available while importance = xl is the least.	Specifies the threshold for tracing messages. All messages beyond the threshold will be traced. Default value is m (medium).
alert	false, true	Specifies to automatically enable trace for severe system events. Default value is true.
severity	'', 'W', 'E', 'A', success, warning, error, assert	Specifies the threshold severity over which messages can be traced. Default value is 'E'.
size	Possible values are integers >= 1000	Specifies the number of messages in a trace log file before a new one is created. Default value is 100000.
keep	false, true	Specifies whether or not to keep the old log file after a new file is created. Default value is false.

Parameter	Possible values	Description
consultant	Strings or integers	Specifies an annotation to use in the output log file. The default value is <blank>. For example, if <pre>consultant = "hello"</pre> this string will be inserted into the log file.
log_dir	String	Specifies the output log file directory. By default log files are stored in the Logging folder. For example, for Windows: <pre>log_dir="C:\Program Files\BusinessObjects Enterprise 12.0\logging"</pre> For UNIX: <pre>log_dir="/usr/bobje/logging"</pre>
always_close	on, off	Specifies if the log file should be closed after a trace is written to the log file. Default value is off.

10. Save and close the BO_trace.ini file.

The settings specified in the BO_trace.ini file override whatever is specified for server tracing in the CMC command line. Your configuration should take affect within a minute of saving the BO_trace.ini file.

Example:

```
active=false;
severity='E';
importance='==';
size=10000000;
keep=false;
```

To configure server tracing through the command line

You can configure server tracing for each BusinessObjects Enterprise server through the CMC by specifying particular parameters in the command line. This approach is used when you want to modify the default location of the server's tracing log file, or to disable tracing.

1. Go to the "Servers" management area of the CMC.
2. Select the server, then choose **Stop Server** from the **Actions** menu.
3. Choose **Properties** from the **Manage** menu.
4. Use the field under "Command Line Parameters" to enter or modify the tracing parameters.

The table below lists all the available parameters for configuring server tracing.

Parameter	Possible values	Description
-trace	off, xs, s, m, l, xl, e, a	Specifies the importance level of messages to trace. The default value is -trace e (i.e. only error messages are traced). If set to -trace xs all messages are traced. Use -trace xl if you want to limit tracing to the most serious/critical messages.
-stackdump	off, on	If set to on, a complete stack trace following a critical error is written to the log file. If no value is specified, stackdump is set to on. The default value is -stackdump off.
-reqtrace	off, on	Records all "Request Trace" messages to the log file and the console in debug builds. Request trace messages include request ID information, therefore a single transaction can be traced through the BusinessObjects Enterprise system across several servers. The default value is -reqtrace off.
-noassert		Turns off SASSERT, SASSERTMSG, SVERIFY, and SASSERTMSG_EX messages. Assert messages will not be written to the log file, and will not appear in the console for debug builds. By default, assert messages are traced.

Parameter	Possible values	Description
-nativeassert	off, on	Turns on/off the native assert behavior for the build architecture. The native assert behavior in debug UNIX builds is to dump core. The native assert behavior in debug Windows builds is to pop up a dialog box with diagnostic information. Both platforms do not trace assert messages in release builds.
-sdktrace	off, on	Specifies whether or not to trace the Business Objects developer libraries. The default value is -sdktrace off.
-filelogfilter		Sets filters for tracing. To trace messages written to a particular set of files, enter a comma-separated list of filenames. To filter out particular files, prefix the comma-separated list of filenames with the ^ character. For example, ^filename1, filename2.
-loggingPath		Specifies the directory where the log file is located. For Windows, the default is the value of the loginPath registry. On UNIX, the default folder is the current working directory - generally the same directory containing the application being traced.
-configFileDir	Full path to BO_trace.ini file.	Specifies the directory hosting the <app_name>_trace.ini file.
-configFile	<app_name>_trace.ini	Specifies the name and location of the trace.ini file.

Parameter	Possible values	Description
-loggingpluginidir		Specifies the directory containing the logging extension DLLs. For Windows, the default is the value of the logginPluginDir registry. On UNIX, the default folder is the current working directory - generally the same directory containing the application being traced.
-alwaysclose	off, on	Specifies if the log file should be closed after a trace is written to the file. The default value is -alwaysclose off.
-nevertrace	off, on	Specifies to turn off tracing. Once tracing is disabled via this option, it cannot be reactivated through the <code><app_name>_trace.ini</code> file. The default value is -nevertrace off.

5. Click **Save & Close**.

6. Restart the server.

Configuring servers for SSL

You can use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your BusinessObjects Enterprise deployment.

To set up SSL for all server communication you need to perform the following steps:

- Deploy BusinessObjects Enterprise with SSL enabled.
- Create key and certificate files for each machine in your deployment.
- Configure the location of these files in the Central Configuration Manager (CCM) and your web application server.

Note:

If you are using thick clients, such as Crystal Reports or Designer you will also need to configure these for SSL if you will be connecting to the CMS from these thick client. Otherwise, you will get errors when you attempt to connect to a CMS that has been configured for SSL from a thick client that has not been configured the same way.

Creating key and certificate files

To set up SSL protocol for your server communication, use the SSLC command line tool to create a key file and a certificate file for each machine in your deployment.

Note:

- You need to create certificates and keys for all machines in the deployment, including machines running thick client components such as Crystal Reports. For these client machines, use the `sslconfig` command line tool to do the configuration.
- For maximum security, all private keys should be protected and should not be transferred through unsecured communication channels.

To create key and certificate files for a machine

1. Run the `SSLC.exe` command line tool.

The SSLC tool is installed with your BusinessObjects Enterprise software. (On Windows, for example, it is installed by default in `C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86.`)

2. Type the following command:

```
sslc req -config sslc.cnf -new -out cacert.req
```

This command creates two files, a Certificate Authority (CA) certificate request (`cacert.req`) and a private key (`privkey.pem`).

3. To decrypt the private key, type the following command:

```
sslc rsa -in privkey.pem -out cakey.pem
```

This command creates the decrypted key, `cakey.pem`.

4. To sign the CA certificate, type the following command:

```
sslc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days
365
```

This command creates a self-signed certificate, `cacert.pem`, that expires after 365 days. Choose the number of days that suits your security needs.

5. Using a text editor, open the `sslc.cnf` file, which is stored in the same folder as the SSLC command line tool.

Note:

Using a text editor is highly recommended for Windows because Windows Explorer may not properly recognize and display files with the .cnf extension.

6. Perform the following steps based on settings in the `ssl.cnf` file.
 - Place the `cakey.pem` and `cacert.pem` files in the directories specified by `ssl.cnf` file's `certificate` and `private_key` options.

By default, the settings in the `sslc.cnf` file are:

```
certificate = $dir/cacert.pem
```

```
private_key = $dir/private/cakey.pem
```

- Create a file with the name specified by the `ssl.cnf` file's database setting.

Note:

By default, this file is `$dir/index.txt`. The file can be empty.

- Create a file with the name specified by the `sslc.cnf` file's `serial` setting.

Ensure that this file provides an octet-string serial number (in hexadecimal format).

Note:

To ensure that you can create and sign more certificates, choose a large hexadecimal number with an even number of digits, such as 11111111111111111111111111111111.'

- Create the directory specified by the `ssl.cnf` file's `new_certs_dir` setting.

7. To create a certificate request and a private key, type the following command:

```
sslc req -config sslc.cnf -new -out servercert.req
```

The certificate and key files generated are placed under the current working folder.

8. Make a copy of the private key.

```
copy privkey.pem server.key
```

9. To sign the certificate with the CA certificate, type the following command:

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

This command creates the servercert.pem file, which contains the signed certificate.

10. Use the following commands to convert the certificates to DER encoded certificates:

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
```

```
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

Note:

The CA certificate (cacert.der) and its corresponding private key (cakey.pem) need to be generated only once per deployment. All machines in the same deployment must share the same CA certificates. All other certificates need to be signed by the private key of any of the CA certificates.

11. Create a text file for storing the plain text `passphrase` used for decrypting the generated private key.
12. Store the following key and certificate files in a secure location (under the same directory) that can be accessed by the machines in your BusinessObjects Enterprise deployment:
 - the trusted certificate file (cacert.der)
 - the generated server certificate file (servercert.der)
 - the server key file (server.key)
 - the passphrase file

This location will be used to configure SSL for the CCM and your web application server.

Configuring the SSL protocol

After you create keys and certificates for each machine in your deployment, and store them in a secure location, you need to provide the Central Configuration Manager (CCM) and your web application server with the secure location.

To configure the SSL protocol in the CCM

1. In the CCM, right-click the Server Intelligence Agent (SIA) and choose **Properties**.
2. In the Properties dialog box, click the **Protocol** tab.
3. Make sure **Enable SSL** is selected, and provide the file path for the directory where you stored the key and certificate files.

Note:

Make sure you provide the directory for the machine that the server is running on.

To configure the SSL protocol on UNIX

You must use the `serverconfig.sh` script to configure the SSL protocol for a SIA. This script provides a text-based program that enables you to view server information and to add and delete servers from your installation. The `serverconfig.sh` script is installed to the `bobje` directory of your installation.

1. Use the `ccm.sh` script to stop the SIA and all the SAP BusinessObjects servers.
2. Run the `serverconfig.sh` script.
3. Select **3 - Modify a Server Intelligence Agent**, and press **Enter**.
4. Specify the target SIA and press **Enter**.
5. Select the **Modify server SSL configuration** option.
6. Select **ssl**.

When prompted specify the SSL certificate locations.

7. Repeat steps 1-6 for every SIA if your SAP BusinessObjects Enterprise deployment is a SIA cluster.
8. Start the SIA with the ccm.sh script, and wait for the servers to start.

To configure the SSL protocol for the web application server

1. If you have a J2EE web application server, run the Java SDK with the following system properties set. For example:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl
-DtrustedCert=cacert.der -DsslCert=clientcert.der -DsslKey=client.key
-Dpassphrase=passphrase.txt
```

The following table shows the descriptions that correspond to these examples:

Example	Description
<code>DcertDir=d:\ssl</code>	The directory to store all the certificates and keys.
<code>DtrustedCert=cacert.der</code>	Trusted certificate file. If specifying more than one, separate with semicolons.
<code>DsslCert=clientcert.der</code>	Certificate used by the SDK.
<code>DsslKey=client.key</code>	Private key of the SDK certificate.
<code>Dpassphrase=passphrase.txt</code>	The file that stores the passphrase for the private key.

2. If you have an IIS web application server, run the `sslconfig` tool from the command line and follow the configuration steps.

Clustering Central Management Servers

If you have a large or mission-critical implementation of BusinessObjects Enterprise, you will probably want to run several CMS machines together in a cluster. A cluster consists of two or more CMS servers working together against a common CMS system database. If a machine that is running one CMS fails, a machine with another CMS will continue to service BusinessObjects Enterprise requests. This "high availability" support helps to ensure that BusinessObjects Enterprise users can still access information when there is an equipment failure.

This section shows how to add a new CMS cluster member to a production system that is already up and running. When you add a new CMS to an existing cluster, you instruct the new CMS to connect to the existing CMS system database and to share the processing workload with any existing CMS machines. For information about your current CMS, go to the Servers management area of the CMC.

Before clustering CMS machines, you must make sure that each CMS is installed on a system that meets the detailed requirements (including version levels and patch levels) for operating system, database server, database access method, database driver, and database client outlined in the `platforms.txt` file included in your product distribution.

In addition, you must meet the following clustering requirements:

- For best performance, the database server that you choose to host the system database must be able to process small queries very quickly. The CMS communicates frequently with the system database and sends it many small queries. If the database server is unable to process these requests in a timely manner, BusinessObjects Enterprise performance will be greatly affected.
- For best performance, run each CMS cluster member on a machine that has the same amount of memory and the same type of CPU.
- Configure each machine similarly:
 - Install the same operating system, including the same version of operating system service packs and patches.
 - Install the same version of BusinessObjects Enterprise (including patches, if applicable).

- Ensure that each CMS connects to the CMS system database in the same manner: whether you use native or ODBC drivers. Make sure that the drivers are the same on each machine, and are a supported version.
- Ensure that each CMS uses the same database client to connect to its system database, and that it is a supported version.
- Check that each CMS uses the same database user account and password to connect to the CMS system database. This account must have create, delete, and update rights on the system database.
- Ensure that the nodes on which each CMS is located are running under the same operating system account. (On Windows, the default is the "LocalSystem" account.)
- Verify that the current date and time are set correctly on each CMS machine (including settings for daylight savings time).
- Ensure that the same .war files are installed on all web application servers in the cluster. For more information on .war file deployment, see the *SAP BusinessObjects Enterprise Installation Guide*.
- Ensure that each and every CMS in a cluster is on the same Local Area Network.
- If your cluster has more than eight CMS cluster members, ensure that the command line for each CMS includes the `-oobthreads <numCMS>` option, where `<numCMS>` is the number of CMS servers in the cluster. This option ensures that the cluster can handle heavy loads. For information about configuring server command lines, see the Server Command Lines appendix of the *SAP BusinessObjects Enterprise Administrator's Guide*.
- If you want to enable auditing, each CMS must be configured to use the same auditing database and to connect to it in the same manner. The requirements for the auditing database are the same as those for the system database in terms of database servers, clients, access methods, drivers, and user IDs.

Tip:

By default, a cluster name reflects the specific name of the first CMS that you install. To modify the default name, see [Changing the name of a CMS cluster](#).

Adding a CMS to a cluster

There are several ways to add a new CMS cluster member. Follow the appropriate procedure:

- If you want to install a new node with a CMS on a new machine, then see [Adding a new node to a cluster](#).
- If you already have a node with CMS binary files, then you can add a new CMS server from the CMC. See [Adding a server](#).
- If you already have a node with CMS binary files, you can also add a new CMS server by cloning an existing CMS server. See [Cloning servers](#).

Note:

Back up your current CMS system database before making any changes. If necessary, contact your database administrator.

Adding a new node to a cluster

When you add a node (a node is a collection of Enterprise servers managed by a single Server Intelligence Agent), you are prompted to either create a new CMS or to cluster the node to an existing CMS. For detailed instructions on adding a node, see [Working with nodes](#).

If you want to cluster a node to an existing CMS, you can also use the installation setup program. Run the BusinessObjects Enterprise installation and setup program on the machine where you want to install the new CMS cluster member. The setup program allows you to perform a Custom installation. During the Custom installation, specify the existing CMS whose system you want to expand, and select the components that you want to install on the local machine. In this case, specify the name of the CMS that is running on your existing system, and choose to install a new CMS on the local machine. Then provide the Setup program with the information it needs to connect to your existing CMS system database. When the Setup program installs the new CMS on the local machine, it automatically adds the server to your existing cluster.

Note:

Before you cluster a new node to an existing CMS, if the new node is a brand new server, ensure that the Enterprise installation on that server is at the same patch level as the existing Enterprise environment.

Adding clusters to the web.xml file

If you have added additional CMSs, and you are using a Java application server, you can modify the `web.xml` file in the `PlatformServices\WEB-INF\` directory of your web application deployment.

To modify the web.xml to define clusters

1. Open the `web.xml`:

In a default deployment on Tomcat 5.5 the file is located in the following directory:

```
C:\Program Files\Business Objects\Tomcat55\webapps\PlatformServices\WEB-INF
```

2. Locate the following section in the file:

```
<!-- EXAMPLE:
    <context-param>
      <param-name>cms.clusters</param-name>
      <param-value>@samplecluster, @samplecluster2,
@samplecluster3</param-value>
    </context-param>
    <context-param>
      <param-name>cms.clusters.samplecluster</param-
name>
      <param-value>cmsone:6400, cmstwo</param-value>
    </context-param>
    <context-param>
      <param-name>cms.clusters.samplecluster2</param-
name>
      <param-value>cms3, cms4, cms5</param-value>
    </context-param>
    <context-param>
      <param-name>cms.clusters.samplecluster3</param-
name>
```

```
<param-value>aps05</param-value>
</context-param>
-->
```

3. Remove the comment tags from this section.
4. In the `param-value` tag under `<param-name>cms.clusters</param-name>`, list the names of each cluster in your deployment.

A “@” character must go before each cluster name in this tag as shown in the example. Separate each cluster name with a comma.

Tip:

Remove the sample cluster names from the section.

5. In the `param-name` tag after the cluster list, type the name of the first cluster .

In the example replace “samplecluster” in

```
<param-name>cms.clusters.samplecluster</param-name>
```

with the cluster name. Cluster names should not include the “@” character in this tag.

6. In the `param-value` tag, list the name of each CMS in the cluster and enter the CMS port number if required.

Note:

Separate each CMS name with a comma. The port number is separated from the CMS name with a colon; The port number is assumed to be 6400 unless a specific port number is provided.

7. Repeat steps 5-6 for each cluster in your deployment.
8. Save your changes.
9. Restart your application server.

Changing the name of a CMS cluster

This procedure allows you to change the name of a cluster that is already installed. After changing the name of the CMS cluster, the Server Intelligences Agent automatically reconfigures each Business Objects server so that it registers with the CMS cluster, rather than with an individual CMS.

Note:

For experienced administrators of BusinessObjects Enterprise, please note that you can no longer use the `-ns` option on the server command line to configure which CMS a server should register with. This is now handled automatically by the SIA.

To change the cluster name on Windows

1. Use the CCM to stop the Server Intelligence Agent for the node that contains a Central Management Server that is a member of the cluster whose name you want to change.
2. Right-click the Server Intelligence Agent and choose **Properties**.
3. In the Properties dialog box, click the **Configuration** tab.
4. Select the **Change Cluster Name to** check box.
5. Type the new name for the cluster.

Note:

Make sure you use a specific CMS name for the cluster. (Do not use the `@cluster` convention used in previous versions of BusinessObjects Enterprise.)

6. Click **OK** and then restart the Server Intelligence Agent.

The CMS cluster name is now changed. All other CMS cluster members are dynamically notified of the new cluster name (although it may take several minutes for your changes to propagate across cluster members).

7. Go to the **Servers** management area of the CMC and check that all of your servers remain enabled. If necessary, enable any servers that have been disabled by your changes.

To change the cluster name on UNIX

Use the `cmsdbsetup.sh` script. For reference, see the Unix Tools chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

Backing up and restoring server configuration settings

The Import Wizard lets you to back up your server configuration settings to a BIAR file, and then use that BIAR to restore those settings at a later date.

Server groups are objects that group related servers together. If you are restoring servers and you are not restoring their related server groups, and the destination system does not contain the same server groups (matched by CUID), you lose the relationship between the server group and the exported server. When you re-import the server, you need to either manually add the server to the desired server groups or create new server groups.

You can set up reports to run on particular server groups. If you are exporting reports and the related server groups are not imported, and do not already exist on the destination, the reports lose their relationship to the server group. If you want the report to use particular server group, and that group does not exist on the destination, you need to manually configure the server groups.

Similarly, if you are importing servers, server groups, or reports without importing the users that have rights on those objects, and those users do not already exist on the destination environment, the rights on those objects are dropped. You may have security settings on those objects that are not correctly set.

Note:

- The Import Wizard supports the backing up and restoring of entire deployments, including all of the servers and nodes in the deployments.
- The Import Wizard Command Line Tool does not support the importing and exporting of server configuration settings.
- If your destination deployment already has servers with the same server identifier as the servers in your BIAR file, then those servers may fail to import. If the import process fails, determine which servers on the destination system have conflicting server identifiers. You can see the server list by viewing the Import Wizard's Detail Log, or by opening the log file `ImportWiz.log`.

If there are servers that conflict because they have the same server identifiers, use the CMC to delete those servers from the destination deployment, and repeat the server import process.

By default, ImportWiz.log is located in C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Logging\

To back up server configuration settings to a BIAR file

1. Specify the BusinessObjects Enterprise XI 3.x system as the source environment.
2. Specify **Business Intelligence Archive Resource (BIAR) File** as the destination environment.
3. On the "Select objects to import" screen, select **Export server configuration**, and click **Next** until the "Ready to Import" screen appears.
4. On the "Ready to Import" screen, click **Finish** to start the import. The "Import Progress" screen appears. After the import is complete, the dialog box displays a summary of the import.
5. Click **Done** to close the Import Wizard.

All of the servers in your BusinessObjects Enterprise deployment are backed up on the BIAR file.

To restore server configuration settings

Before you restore the server configuration settings from a BIAR file, you should first backup your existing configuration. Once you restore the configuration settings, the only way to revert back to the state before the restore is by importing the settings from the second BIAR file.

It is recommended that when you add or delete a BusinessObjects Enterprise server from a BusinessObjects Enterprise cluster, you export the server configuration settings for the entire cluster to a BIAR file. This prevents a situation where the cluster contains more servers than the BIAR file that you are importing from does, so that you do not have to manually delete the servers before restoring your server configuration settings from the BIAR file.

Note:

- If you've created additional servers or nodes after you backed up your configuration settings, and use the Import Wizard to restore the configuration settings, the Import Wizard doesn't update or delete these servers or nodes. However if such servers used configuration templates then they can become reconfigured. This is because during restore process the configuration templates are updated, affecting the server's configuration. If you want to get your system to the same server configuration state as it was at the time of the backup, and your BusinessObjects Enterprise deployment has more servers than the BIAR file that you are restoring from does, you may want to delete the servers through the CMC before you restore. If you delete servers from your BusinessObjects Enterprise deployment, you must ensure that the deployment has at least one CMS to run the Import Wizard.
 - Do not restore server configuration settings from a Windows deployment to a UNIX deployment or from a UNIX deployment on a Windows deployment. Always restore server configuration settings from a Windows deployment to a Windows deployment and from Unix deployment to Unix deployment.
1. Specify the BIAR file that contains the server configuration settings that you want to import as the source environment.
 2. Specify your BusinessObjects Enterprise XI 3.x system as the destination environment.
 3. On the "Select objects to import" screen, select **Restore Full Cluster Server Configuration**, and click **Next**.

Note:

If you select **Import node(s) from a different cluster**, you can't select **Restore Full Cluster Server Configuration**.

4. On the "Import Scenarios" screen, specify what you want the Import Wizard to do if it finds an object with the same unique identifier on the destination environment.

Note:

When you are importing objects from a BIAR file, the option to match objects by name and path is not available.

The options that you can select are:

- **Update the destination object, in case of name conflict, rename it.**

Use this option when you want to restore all server objects that are in a BIAR file to a deployment. If the deployment already has other servers with the same names, then some of the updated servers may be renamed.

If a server in the BIAR files has a unique identifier that matches a server's unique identifier on the deployment, then the server on the deployment will be overwritten with the configuration settings of the server located in the BIAR file.

If, during the import process, the Import Wizard discovers that the deployment already has another server with the same name as the server from the BIAR file, the Import Wizard imports the server and renames it. The server's new name will be server name as it appears in the BIAR file, appended with a number in brackets.

- **Update the destination object, in case of name conflict, do not rename it.**

Use this option when you want to restore all server objects from the BIAR file to a deployment, except the servers with different unique identifiers but with the same names.

- **Do not import the object**

Use this option if you do not want servers on deployment to be overwritten with settings from the BIAR file. This will cause only servers not existing on your deployment (but existing in the BIAR file) to be restored.

See [Restoring server configuration scenarios](#) for examples that describe how server configuration settings can be restored from BIAR files.

5. On the "Incremental import" screen, select whether you want to overwrite object contents or overwrite right contents.
6. Click **Next** until the "Ready to Import" screen appears.
7. On the "Ready to Import" screen, click **Finish**.
The "Import Progress" screen appears. After the import is complete, the screen displays a summary of the import.
8. Click **Done** to close the Import Wizard.

Restoring server configuration scenarios

This section describes scenarios for using the Import Wizard to restore server configuration settings from a BIAR file, and illustrates how selecting different import scenarios affects how server settings are imported.

For all of the scenarios, the initial configuration is described in the following tables.

Table 5-7: Initial Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.cms	1	Request Port	6401
mynode.eventserver	2	Maximum Idle Time	2

When you export these settings to a BIAR file, the file contains the same server settings.

Table 5-8: Initial Server Configuration Settings in the BIAR file

Server Name	Unique Identifier	Property	Value
mynode.cms	1	Request Port	6401
mynode.eventserver	2	Maximum Idle Time	2

All of the following scenarios assume that we are importing the server configuration settings from this BIAR file.

Suppose that you modify the server configuration settings on the deployment so that the deployment now has the configuration settings described in the following table.

Table 5-9: New Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.cms	1	Request Port	6402
mynode.eventserver	2	Maximum Idle Time	3

The following two scenarios describe how the options on the "Import scenario" screen affect the process of restoring server configuration settings from the BIAR file.

Scenario 1

This scenario describes what the Import Wizard does when, on the Import scenario screen, you select **Use the object's unique identifier to determine whether it already exists in the destination system**, and then select one of the following options.

- **Update the destination object. In case of name conflict, rename it,**
or
- **Update the destination object. In case of name conflict, do not import it.**

The deployment's initial configuration settings are described in the following table.

Table 5-10: Initial Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.cms	1	Request Port	6402

Server Name	Unique Identifier	Property	Value
mynode.eventserver	2	Maximum Idle Time	3

When you import the servers from the BIAR file, the Import Wizard finds servers in the BIAR file and on the deployment with matching unique identifiers. The Import Wizard overwrites the values on the deployment with the values from the BIAR file. In other words, the deployment's original settings are restored.

The server configuration settings on the deployment after this workflow are described in the following table.

Table 5-11: New Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.cms	1	Request Port	6401
mynode.eventserver	2	Maximum Idle Time	2

Scenario 2

This example explains what happens when, on the Import scenario screen, you select the **Use the object's unique identifier to determine whether it already exists in the destination system.** and **Do not import the object** options.

The deployment's initial configuration settings are described in the following table.

Table 5-12: Initial Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.cms	1	Request Port	6402
mynode.eventserver	2	Maximum Idle Time	3

When you match by unique identifier and choose the **Do not import the object** option, the Import Wizard finds servers with the matching unique identifiers, and does not import the server configuration settings. The servers on the deployment are not updated.

Scenario 3

The following examples show what happens when you modify the server configuration settings on the deployment, and then try to restore the settings from the BIAR file that you imported the settings to. Suppose that you make the following three changes on the deployment.

- Rename the mynode.cms server to mynode.primarycms.
- Add a new server, called mynode.cms, with the Request Port property set to 6404.

When a new server is added, it is automatically assigned a new unique identifier.

- Delete the event server.

The following table describes the server settings on the destination deployment after these modifications.

Table 5-13: Server Configuration Settings on the Destination Deployment

Server Name	Unique Identifier	Property	Value
mynode.primarycms	1	Request Port	6402
mynode.cms	3	Request Port	6404

When you restore the server configuration settings from the BIAR file, the particular settings that are imported to the deployment depends on the options that you select on the "Import scenarios" screen.

Scenario 3.1

Suppose that you use the Import Wizard to restore the server configuration settings from the BIAR file, and that on the Import scenarios screen, you select **Use the object's unique identifier to determine whether it already exists in the destination system** and **Update the destination object, in case of name conflict, rename it**.

Use this option when you want to restore all servers from a BIAR file to a deployment.

The deployment's initial configuration settings are described in the following table.

Table 5-14: Initial Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.primarycms	1	Request Port	6402
mynode.cms	3	Request Port	6404

When you match by unique identifier and choose the **Update the destination object, in case of name conflict, rename it** option, the Import Wizard finds that the unique identifier for mynode.cms from BIAR is 1, and that the unique identifier of the mynode.primarycms server on the deployment is also 1. However, when it detects that the deployment already has another server with mynode.cms name, it renames the restored server.

Furthermore, because the mynode.cms server doesn't exist in the BIAR file, that server is not updated during the import process.

This results in the deployment described in the following table.

Table 5-15: Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value	Result
mynode.cms(2)	1	Request Port	6401	This server is restored with a new name.
mynode.eventserver	2	Maximum Idle Time	2	This server is restored.
mynode.cms	3	Request Port	6404	This server is not updated, because it does not exist in the BIAR file.

Scenario 3.2

Suppose that you use the Import Wizard to restore the server configuration settings from the BIAR file, and that on the Import scenarios screen, you select **Use the object's unique identifier to determine whether it already exists in the destination system** and **Update the destination object, in case of name conflict, do not import it**.

Use this option when you want to restore all server objects from a BIAR file to a deployment, except servers with different unique identifiers but with the same name.

The deployment's initial configuration settings are described in the following table.

Table 5-16: Initial Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.primarycms	1	Request Port	6402
mynode.cms	3	Request Port	6404

When you match by unique identifier and choose the **Update the destination object, in case of name conflict, do not import it** option, the Import Wizard does not import the server settings from the BIAR file for mynode.cms, even though the unique identifiers of mynode.cms (in the BIAR file) and mynode.primarycms (on the deployment) are the same. This is because the Import Wizard detects a server on the destination with the same name, and does not import the server.

The results in the deployment are described in the following table.

Table 5-17: Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value	Result
mynode.primarycms	1	Request Port	6402	This server is not updated.
mynode.eventserver	2	Maximum Idle Time	2	This server is restored.

Server Name	Unique Identifier	Property	Value	Result
mynode.cms	3	Request Port	6404	This server is not updated, because it does not exist in the BIAR file.

Scenario 3.3

Suppose that you use the Import Wizard to restore the server configuration settings from the BIAR file, and that on the Import scenarios screen, you select **Use the object's unique identifier to determine whether it already exists in the destination system** and **Do not import the object** on the "Import scenario" screen.

Use this option when you do not want the servers on a deployment to be overwritten by servers from a BIAR file. This option only restores servers that do not exist on the deployment, but that are in the BIAR file.

The deployment's initial configuration settings are described in the following table.

Table 5-18: Initial Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value
mynode.primarycms	1	Request Port	6402
mynode.cms	3	Request Port	6404

When you match by unique identifier and choose the **Do not import the object** option, the Import Wizard does not import the server settings from the BIAR file for mynode.cms, even though the unique identifiers of mynode.cms (on the BIAR file) and mynode.primarycms (on the destination environment) match. This is because you've selected to not import objects where the source and destination environments have the same unique identifier.

The results in the deployment are described in the following table.

Table 5-19: Server Configuration Settings on the Deployment

Server Name	Unique Identifier	Property	Value	Result
mynode.primarycms	1	Request Port	6402	This server is not updated, because you've chosen not to overwrite existing servers on the deployment.
mynode.eventserver	2	Maximum Idle Time	2	This server is restored.
mynode.cms	3	Request Port	6404	This server is not updated, because it does not exist in the BIAR file.

To import nodes from one cluster to another

There are a number of situations that may require you to re-point existing nodes to different clusters. For example, if you want to add a node to a Production deployment, and want to make the change as smooth as possible, you may want to create the node on a Test deployment, and then re-point it to the Production deployment. Direct migration of nodes between deployments is not supported in BusinessObjects Enterprise XI 3.x, in favor of a more secure method involving import and export of server configuration settings.

In BusinessObjects Enterprise XI 3.x, server configuration information is stored in the CMS database, so instead of moving the node between deployments, you import the server configuration settings from one deployment to the other. You need to first import the node's configuration information to the destination node. You can then re-point the node (Server Intelligence Agent) to the destination cluster.

Note:

If you are importing nodes from one cluster to another, the Import Wizard does not import configuration templates from BIAR files.

To re-point a node on a Test deployment so that the node joins the cluster on the Production deployment:

1. On the Test deployment, start the Import Wizard and export the server configuration settings to a BIAR file. For information on importing nodes to a BIAR file, see *To back up server configuration settings to a BIAR file*.
2. On the Test deployment, stop the Server Intelligence Agent .
3. On the Production deployment , use the Import Wizard to import the node from the BIAR file.
 - a. Start the Import Wizard.
 - b. Select the BIAR file that contains the node as the source environment.
 - c. On the "Select objects to import" screen, select **Import node(s) from a different cluster** , and click Next.
 - d. On the "Import scenario" screen, select what you want the Import Wizard to do if it finds any objects on the destination environment with the same unique identifier.
 - e. On the "Incremental import" screen, select whether you want the Import Wizard to overwrite any objects or object rights that already exist on the destination environment.

- f. On the "Nodes" screen, select the node that you want to import, and click **Next**.
- g. On the "Ready to Import" screen, click **Finish**.
- h. On the "Import Progress" screen, click **Done**.
4. If you are not re-pointing all of the nodes that are on the Test deployment, then reconfigure the Test deployment's node that you are re-pointing:
 - If you are re-pointing a node on a Windows deployment, follow these steps.
 - a. On the Test deployment, start the CCM.
 - b. Right-click the node that you imported to the Production environment, and select **Properties > Startup**.
 A list of local and remote CMS Servers is displayed.
 - c. Click **Remove**, to remove the link to the CMSs that you are not re-pointing.
 - d. Click **OK**.
 - If you are re-pointing a node on a UNIX deployment, run the `serverconfig.sh` script to remove the link to the CMSs that you are not re-pointing.
5. If the node that you've imported contains a CMS:
 - On Windows, perform the following steps.
 - a. On the Test deployment, start the CCM.
 - b. Right-click the Server Intelligence Agent for the node that you are re-pointing, and select **Properties > Configuration**.
 - c. Click **Select a Data Source**.
 - d. Type the DSN for the Production database, and click **OK**.
 - On Unix, run the `cmsdbsetup.sh` script to change the node's data source to the Production database.
6. On the Test deployment, start the re-pointed Server Intelligence Agent.

Related Topics

- [To back up server configuration settings to a BIAR file](#)



Configuring Third-Party Authentication

6

chapter



This section provides detailed instructions for configuring BusinessObjects Enterprise to work with third-party authentication options.

Using NT Authentication

This section provides a general description of how NT authentication works with BusinessObjects Enterprise. It then introduces the administration tools that allow you to manage and configure NT user accounts to BusinessObjects Enterprise.

Related Topics

- [Using NT user accounts and groups](#)
- [Windows NT security plug-in](#)
- [NT user account and group administration](#)
- [Mapping NT user accounts and groups](#)

Using NT user accounts and groups

BusinessObjects Enterprise supports NT authentication with the Windows NT security plug-in, which is included by default when the product is installed on Windows. Support for NT authentication means that users or groups created with NT, Windows 2000 and Windows 2003 can be used to authenticate with BusinessObjects Enterprise. This allows you to map previously created NT user accounts and groups, instead of setting up each user and group within BusinessObjects Enterprise.

Windows NT security plug-in

The Windows NT security plug-in (`secWindowsNT.dll`) allows you to map user accounts and groups from your Windows NT user database to BusinessObjects Enterprise; it also enables BusinessObjects Enterprise to verify all logon requests that specify Windows NT Authentication. Users are authenticated against the Windows NT user database, and have their membership in a mapped NT group verified before the CMS grants them an active BusinessObjects Enterprise session.

This plug-in is compatible with NT 4 and Windows 2000 Active Directory user databases (when Windows 2000 Active Directory is configured in non-native mode only). If a Windows 2000 Active Directory user database is configured in native mode and contains universal groups that span several domains, you must use the Windows AD security plug-in. For information on mapping Windows NT users and groups to BusinessObjects Enterprise, see [Mapping NT user accounts and groups](#). For information on the Windows AD security plug-in, see [Windows AD security plug-in](#).

Once you have mapped your NT users and groups, all Windows-based BusinessObjects Enterprise client tools support NT authentication, while Java-based tools do not. You can also create your own applications that support NT authentication. For more information, see the developer documentation available on your product CD.

Note:

The Windows NT security plug-in cannot authenticate users under the following conditions:

- If the BusinessObjects Enterprise server components are running on UNIX.
- If your system uses the BusinessObjects Enterprise Java SDK.

Note:

The CMC and other Java-based applications do not support NT authentication.

NT user account and group administration

Setting up and maintaining NT authentication involves these tasks:

- [Mapping NT groups from the CMC](#)
- [Unmapping NT groups](#)
- [Viewing mapped NT users and groups](#)

Mapping NT user accounts and groups

To simplify administration, BusinessObjects Enterprise supports user accounts and groups that are created using Windows NT. However, before users can use their NT user name and password to log on to BusinessObjects Enterprise, their NT user account needs to be mapped to BusinessObjects Enterprise. When you map an NT account, you can choose to create a new BusinessObjects Enterprise account or link to an existing BusinessObjects Enterprise account.

You can map NT accounts to BusinessObjects Enterprise through the CMC.

Note:

NT accounts refer to Windows NT, 2000 and 2003 accounts.

Mapping NT groups from the CMC

To simplify administration, BusinessObjects Enterprise supports user accounts and groups that are created using Windows NT. However, before users can use their NT user name and password to log on to BusinessObjects Enterprise, their NT user account needs to be mapped to BusinessObjects Enterprise. When you map an NT account, you can choose to create a new BusinessObjects Enterprise account or link to an existing BusinessObjects Enterprise account.

Note:

- When you map a NT group to BusinessObjects Enterprise, all the users from the group are mapped. If you want to exclude specific users from having access to BusinessObjects Enterprise, you can change the specific user's access after the group has been mapped.
- Before starting this procedure, ensure you have the NT domain and group information.

To map NT groups using BusinessObjects Enterprise

1. Go to the **Authentication** management area of the CMC.
2. Double-click **Windows NT**.
3. Ensure that the **NT Authentication is enabled** check box is selected.
4. If you will be using single sign-on, select the **Single Sign On is enabled** check box.

Note:

If you select this option, you must also configure the IIS for single sign-on. For details, see [Setting up NT single sign-on](#). Failing to configure IIS could compromise your system security if the account that IIS runs under belongs to a mapped group, because users who use one of the web applications would automatically have the same access privileges as the IIS machine account.

5. To change the Default NT domain, click the domain name. Complete the **Default NT Domain** field.

Note:

By typing the default NT Domain Name, users do not have to specify the NT Domain Name when they log on to BusinessObjects Enterprise via NT authentication. Also, you don't have to specify the NT domain name when you map groups.

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

Note:

If you want to map a local NT group, you must type \\NTmachine name\groupname.

7. Click **Add**.

The group is added to the list.

8. Select how aliases are mapped to BusinessObjects Enterprise accounts.
 - a. In "New Alias Options", select how new aliases are mapped to Enterprise accounts. Select one of the following choices:

- **Assign each added NT 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, NT 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 NT account, are added as new users.

- **Create a new account for every added NT 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 NT user mapped to BusinessObjects Enterprise. New NT accounts are added for users without BusinessObjects Enterprise accounts, or for all users if you selected the **Create a new account for every added NT alias** option.

- **Create new aliases only when the user logs on**

Use this option when the NT directory you are mapping contains many users, but only a few of them will use BusinessObjects Enterprise. BusinessObjects Enterprise 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 BusinessObjects Enterprise.

- 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise, a 100 user concurrent license could support 250, 500, or 700 users.

9. Click **Update**.

Unmapping NT groups

Similar to mapping, it is possible to unmap groups using the administrative tool in Windows NT/2000, or BusinessObjects Enterprise.

To unmap NT users and groups using Windows NT

1. From the Administrative Tools program group, click **User Manager**.
2. Select the group containing the users you want to unmap.
3. From the **User** menu, click **Properties**.
4. Select the user(s) or group(s), and click **Remove**.
5. Click **OK**.

The user or group will no longer be able to access BusinessObjects Enterprise.

Note:

If you remove a user from an NT group, the NT alias for that user is also removed from BusinessObjects Enterprise. If the removed alias is the only one the user has, the user and its Favorites, Inbox and all other personal content are also removed from BusinessObjects Enterprise.

To unmap NT users and groups using Windows 2000 or 2003

1. From the Administrative Tools program group, click **Computer Management**.
2. Under **System Tools**, select **Local Users and Groups**.
3. Click the **Groups** folder.
4. Select the group containing the users you want to unmap.
5. From the **Action** menu, click **Properties**.
6. Select the user(s) or group(s), and click **Remove**.
7. Click **OK** or **Apply** (and then **Close**) to complete the process.

The user or group will no longer be able to access BusinessObjects Enterprise.

Note:

If you remove a user from a Windows 2000 or Windows 2003 group, the NT alias for that user is also removed from BusinessObjects Enterprise. If the removed alias is the only one the user has, the user and its

Favorites, Inbox and all other personal content are also removed from BusinessObjects Enterprise.

To unmap NT groups using BusinessObjects Enterprise

1. Go to the **Authentication** management area of the CMC.
2. Double-click **Windows NT**.
3. In the Mapped NT Member Groups area, select the NT group you would like to remove.
4. Click **Delete**.
5. Click **Update**.

The users in this group will not be able to access BusinessObjects Enterprise.

Tip:

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

Note:

If you unmap an NT group from BusinessObjects Enterprise, the NT alias for all the users in the group will also be removed from BusinessObjects Enterprise. If the removed alias is the only one for these user, the users and their Favorites, Inbox and all other personal content are also removed from BusinessObjects Enterprise.

Viewing mapped NT users and groups

There are two methods to view mapped users and groups in BusinessObjects Enterprise.

Note:

When you view group membership, the information is cached. If you add more users to the mapped group, they will appear when the cache expires (10 minutes, by default) or when the CMS restarts.

To view users and groups that have been added using Windows NT/2000, 2003 or BusinessObjects Enterprise

1. Go to the **Users** management area of the CMC.
2. Select the appropriate group.

3. Click **OK** to the message which states that accessing the user list may take several seconds.
4. Click **Refresh**, then click **OK**.

To view groups that have been added using BusinessObjects Enterprise

1. Go to the **Authentication** management area of the CMC.
2. Double click **Windows NT**.

The "Mapped NT Member Groups" area displays the groups that have been mapped to BusinessObjects Enterprise.

Note:

You can view the groups and users by selecting the appropriate group from the Users management area.

Adding an NT account to a mapped NT group

When you have added a new account in NT, and the NT group to which the account belongs to is already mapped to BusinessObjects Enterprise, there are three ways you can get the new NT account into BusinessObjects Enterprise. Choose the method that works best for your situation:

- When the new NT user logs on to BusinessObjects Enterprise and selects NT authentication, the system will add the user to BusinessObjects Enterprise. This is the simplest method and it doesn't require any extra steps, but the user won't be added until he or she logs on to BusinessObjects Enterprise.
- You can add the new user to BusinessObjects Enterprise and select Windows NT authentication. The user is added and is automatically assigned a Windows NT alias. For more information on aliases, see [Security Concepts](#).
- You can go to the Windows NT tab in the Authentication management area and select the option to add all new aliases and create all new users, and then click **Update**. In this case all NT users will be added to BusinessObjects Enterprise. For details, see [Mapping NT user accounts and groups](#). However, if the NT group contains many users who don't require access to BusinessObjects Enterprise, you may want to add the user individually instead.

Creating a new NT group account

- If you create a new NT group account, and the group account does not belong to a group account that is mapped to BusinessObjects Enterprise, add it to BusinessObjects Enterprise. For more information, see [Mapping NT user accounts and groups](#).
- If you create a new NT group account, and the account belongs to a group account that is mapped to BusinessObjects Enterprise, refresh the group list. For more information, see [Viewing mapped NT users and groups](#).

Disabling an NT user account

If you disable an NT user account (using Windows Administrative Tools), the user will not be able to log on to BusinessObjects Enterprise using the mapped NT account. However, if the user also has an account that uses Enterprise authentication, the user can still access BusinessObjects Enterprise using that account.

Setting up NT single sign-on

You can configure BusinessObjects Enterprise to allow users to use various BusinessObjects Enterprise applications without being prompted to log on. Users need only to enter their NT user name and password information once at the beginning of the NT session. For instance, if you have set up NT single sign-on, when you launch InfoView, NT authentication occurs in the background. You are not required to enter any additional information.

Note:

This feature is available if you are using a Microsoft Internet Information Server (IIS) and the users are using Internet Explorer as their web browser. For specific version compatibility, refer to the BusinessObjects Enterprise supported platform document (PAR) on our support web site: http://support.businessobjects.com/documentation/supported_platforms.

BusinessObjects Enterprise provides its own form of "anonymous single sign-on," which uses Enterprise authentication, as opposed to Windows NT authentication. Design your own web applications accordingly (or modify InfoView) if you want to use NT single sign-on. Refer to the tutorial in the developer documentation for an example on creating a web application that uses single sign-on.

Setting up NT single sign-on to BusinessObjects Enterprise includes these tasks:

- [Modifying the web.config file for NT single sign-on](#)
- [Enabling InfoView NT single sign-on from the CMC](#)

Enabling InfoView NT single sign-on from the CMC

To enable the Windows NT plug-in for single sign-on from the CMC

1. Go to the **Authentication** management area of the CMC.
2. Double-click **Windows NT**.
3. Select the **Single Sign On is enabled** check box.

Note:

If you select this option, you must also configure the IIS for single sign-on. For details, see [Modifying the web.config file for NT single sign-on](#). Failing to configure IIS could compromise your system security if the account that IIS runs under belongs to a mapped group, because when users access one of the web applications they would automatically have the same access privileges as the IIS machine account.

4. Click **Update**.

Note:

For NT single sign-on to function correctly, make sure you complete all tasks listed in [Setting up NT single sign-on](#).

To modify the security setting on IIS

1. From the Windows Administrative Tools program group, click **Computer Management**.
2. Expand **Services and Applications**.
3. Expand **Internet Information Services**.
4. Click on the web site that runs InfoView, and then select **Properties**.
5. Click on the **Directory Security** tab.
6. In the Anonymous access and authentication control area of the page, click **Edit**.
7. Deselect the **Anonymous access** and **Basic authentication** check boxes.
8. Ensure that the **Integrated Windows authentication** check box is selected.

9. Click **OK**.
10. Click **OK**.
11. Restart your IIS server.

Modifying the web.config file for NT single sign-on

To configure InfoView for single sign-on, you must modify its associated `web.config` file in the `InfoViewApp` directory.

To modify the web.config file for NT single sign-on

1. Open the appropriate `web.config` file from this location:
C:\Program Files\Business Objects\BusinessObjects
Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp\

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Locate the following line in the `<system.web>` block:

```
<Authentication mode="None" />
```

3. Replace "None" with "Windows".

```
<Authentication mode="Windows" />
```

4. Add the following line:

```
<identity impersonate="true" />
```

5. Find the following string:

```
<add key="cmsDefault" value="" />
```

6. Enter the CMS machine in the `cmsDefault` value field.

7. Find the following string:

```
<add key=" ssoEnabled" value="false" />
```

8. Change the `ssoEnabled` value from `false` to `true`.
9. Find the following string:

```
<add key="authenticationDefault" value="secEnterprise" />
```

10. Ensure the value for `authenticationDefault` is set to `secWindows NT`.
11. Save and close the file.
12. Restart IIS.

Using LDAP authentication

This section provides a general description of how LDAP authentication works with BusinessObjects Enterprise. It then introduces the administration tools that allow you to manage and configure LDAP accounts to BusinessObjects Enterprise.

Related Topics

- [Managing LDAP accounts](#)
- [Configuring LDAP authentication](#)
- [Mapping LDAP groups](#)
- [Unmapping LDAP groups](#)
- [Viewing mapped LDAP users and groups](#)
- [Changing LDAP connection parameters and member groups](#)
- [Managing multiple LDAP hosts](#)
- [Troubleshooting LDAP accounts](#)

Managing LDAP accounts

To use LDAP authentication, you need to first ensure that you have your respective LDAP directory set up. For more information about LDAP, refer to your LDAP documentation. For more information on the LDAP security plug-in, see [LDAP security plug-in](#).

Note:

When you install BusinessObjects Enterprise, the LDAP authentication plug-in is installed automatically, but not enabled by default.

Related Topics

- [Configuring LDAP authentication](#)
- [Mapping LDAP groups](#)
- [Unmapping LDAP groups](#)
- [Viewing mapped LDAP users and groups](#)
- [Changing LDAP connection parameters and member groups](#)
- [Managing multiple LDAP hosts](#)
- [Troubleshooting LDAP accounts](#)

LDAP security plug-in

The LDAP security plug-in (`secLDAP.dll`) allows you to map user accounts and groups from your LDAP directory server to BusinessObjects Enterprise; it also enables the system to verify all logon requests that specify LDAP authentication. Users are authenticated against the LDAP directory server, and have their membership in a mapped LDAP group verified before the CMS grants them an active BusinessObjects Enterprise session. User lists and group memberships are dynamically maintained by BusinessObjects Enterprise. You can specify that BusinessObjects Enterprise use a Secure Sockets Layer (SSL) connection to communicate to the LDAP directory server for additional security.

LDAP authentication for BusinessObjects Enterprise is similar to NT and AD authentication in that you can map groups and set up authentication, authorization, and alias creation. Also as with NT or AD authentication, you can create new Enterprise accounts for existing LDAP users, and can assign LDAP aliases to existing users if the user names match the Enterprise user names. In addition, you can do the following:

- Map users and groups from the LDAP directory service.
- Map LDAP against AD. There are a number of restrictions if you configure LDAP against AD. For details, see [Mapping LDAP against AD](#).
- Specify multiple host names and their ports.
- Configure LDAP with SiteMinder.

For information on mapping your LDAP users and groups to BusinessObjects Enterprise, see [Managing LDAP accounts](#).

Once you have mapped your LDAP users and groups, all of the BusinessObjects Enterprise client tools support LDAP authentication. You can also create your own applications that support LDAP authentication.

More about LDAP

Lightweight Directory Access Protocol (LDAP), a common, application-independent directory, enables users to share information among various applications. Based on an open standard, LDAP provides a means for accessing and updating information in a directory.

LDAP is based on the X.500 standard, which uses a directory access protocol (DAP) to communicate between a directory client and a directory server. LDAP is an alternative to DAP because it uses fewer resources and simplifies and omits some X.500 operations and features.

The directory structure within LDAP has entries arranged in a specific schema. Each entry is identified by its corresponding distinguished name (DN) or common name (CN). Other common attributes include the organizational unit name (OU), and the organization name (O). For example, a member group may be located in a directory tree as follows: cn=BusinessObjects Enterprise Users, ou=Enterprise Users A, o=Research. Refer to your LDAP documentation for more information.

Because LDAP is application-independent, any client with the proper authorization can access its directories. LDAP offers you the ability to set up users to log on to BusinessObjects Enterprise through LDAP authentication. It also enables users to be authorized when attempting to access objects in BusinessObjects Enterprise. As long as you have an LDAP server (or servers) running, and use LDAP in your existing networked computer systems, you can use LDAP authentication (along with Enterprise, NT, and Windows AD authentication).

If desired, the LDAP security plug-in provided with BusinessObjects Enterprise can communicate with your LDAP server using an SSL connection established using either server authentication or mutual authentication. With server authentication, the LDAP server has a security certificate which BusinessObjects Enterprise uses to verify that it trusts the server, while the LDAP server allows connections from anonymous clients. With mutual authentication, both the LDAP server and BusinessObjects Enterprise have security certificates, and the LDAP server must also verify the client certificate before a connection can be established.

The LDAP security plug-in provided with BusinessObjects Enterprise can be configured to communicate with your LDAP server via SSL, but always performs basic authentication when verifying users' credentials. Before deploying LDAP authentication in conjunction with BusinessObjects Enterprise, ensure that you are familiar with the differences between these LDAP types. For details, see RFC2251, which is currently available at <http://www.faqs.org/rfcs/rfc2251.html>

Mapping LDAP against AD

If you configure LDAP against AD, note the following restrictions:

- If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.
- Users who are only members of default groups from AD will not be able to log in successfully. Users must also be a member of another explicitly created group in AD and, in addition, this group must be mapped. An example of such a group is the "domain users" group.
- If a mapped domain local group contains a user from a different domain in the forest, the user from a different domain in the forest will not be able to log in successfully.
- Users from a universal group from a domain different than the DC specified as the LDAP host will not be able to log in successfully.
- You cannot use the LDAP plug-in to map users and groups from AD forests outside the forest where BusinessObjects Enterprise is installed.
- You cannot map in the Domain Users group in AD.
- You cannot map a machine local group.
- If you are using the Global Catalog Domain Controller, there are additional considerations when mapping LDAP against AD:

Situation	Considerations
Multiple domains when pointing to the Global Catalog Domain Controller	<p>You can map in:</p> <ul style="list-style-type: none"> • universal groups on a child domain, • groups on the same domain that contains universal groups from a child domain, and • universal groups on a cross domain. <p>You cannot map in:</p> <ul style="list-style-type: none"> • global groups on a child domain, • local groups on a child domain, • groups on the same domain that contain a global group from the child domain, and • cross-domain global groups. <p>Generally, if the group is a universal group, it will support users from cross or child domains. Other groups will not be mapped if they contain users from cross or child domains. Within the domain you are pointing to, you can map domain local, global, and universal groups.</p>
Mapping in universal groups	<p>To map in universal groups, you must point to the Global Catalog Domain Controller. You should also use port number 3268 instead of the default 389.</p>

- If you are using multiple domains but not pointing to the Global Catalog Domain Controller, then you cannot map in any type of groups from cross or child domains. You can map in all types of groups only from the specific domain you are pointing to.

Configuring LDAP authentication

To simplify administration, BusinessObjects Enterprise supports LDAP authentication for user and group accounts. Before users can use their LDAP user name and password to log on to BusinessObjects Enterprise, you need to map their LDAP account to BusinessObjects Enterprise. When you map an LDAP account, you can choose to create a new BusinessObjects Enterprise account or link to an existing BusinessObjects 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.

Configuring LDAP authentication includes the following steps:

- [Configuring the LDAP host.](#)
- [Configuring LDAP Server or Mutual Authentication and the SSL settings.](#)
- [Configuring the LDAP plug-in for SiteMinder.](#)

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.

Configuring the LDAP host

To configure the LDAP host

1. Go to the **Authentication** management area of the CMC, and then double-click **LDAP**.

Note:

To get to the **Authentication** management area, choose **Authentication** from the navigation list.

2. 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 **OK**.

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**. For more information on multiple hosts, refer to [Managing multiple LDAP hosts](#).

3. Select your server type from the **LDAP Server Type** list.

Note:

If you are Mapping LDAP to AD, select Microsoft Active Directory Application Server for your server type.

4. If you want to view or change any of the LDAP Server Attribute Mappings or the LDAP Default Search Attributes, click **Show Attribute Mappings**.

By default, each supported server type's server attribute mappings and search attributes are already set.

5. Click **Next**.

6. In the **Base LDAP Distinguished Name** field, type the distinguished name (for example, o=SomeBase) for your LDAP server, and then click **Next**.

7. In the LDAP Server Credentials area, specify the distinguished name and password for a user account that has read access to the directory.

Note:

Administrator credentials are not required.

Note:

If your LDAP Server allows anonymous binding, leave this area blank—BusinessObjects Enterprise servers and clients will bind to the primary host via anonymous logon.

8. If you have configured referrals on your LDAP host, enter the authentication information in the **LDAP Referral Credentials** area, and then enter the number of referral hops in the **Maximum Referral Hops** field.

Note:

The "LDAP Referral Credentials" area must be configured if all of the following 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 BusinessObjects Enterprise.

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.
- If "Maximum Referral Hops" is set to zero, no referrals will be followed.

9. Click **Next**.

10. Choose the type of Secure Sockets Layer (SSL) authentication used, and then click **Next**.

These are your choices:

- Basic (no SSL)
- Server Authentication
- Mutual Authentication

Note:

See [Configuring LDAP Server or Mutual Authentication and the SSL settings](#) for further information.

11. Choose a method of LDAP single sign-on authentication, and then click **Next**.

These are your choices:

- Basic (No SSO)
- SiteMinder

Note:

If you select SiteMinder, see [Configuring the LDAP plug-in for SiteMinder](#).

12. Select how aliases are mapped to BusinessObjects Enterprise accounts.

- a. In "New Alias Options", select how new aliases are mapped to Enterprise accounts. Select one of the following choices:
 - **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 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 "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 LDAP user mapped to BusinessObjects Enterprise. New LDAP accounts are added for users without BusinessObjects Enterprise accounts, or for all users if you selected the **Create a new account for every added LDAP alias** option.

- **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 BusinessObjects Enterprise. BusinessObjects Enterprise 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 BusinessObjects Enterprise.

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 BusinessObjects Enterprise 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 BusinessObjects Enterprise, a 100 user concurrent license could support 250, 500, or 700 users.

13. Click *Finish*.

Managing multiple LDAP hosts

Using LDAP and BusinessObjects Enterprise, you can add fault tolerance to your system by adding multiple LDAP hosts. BusinessObjects Enterprise uses the first host that you add as the primary LDAP host. Subsequent hosts are treated as failover hosts.

The primary LDAP host and all failover hosts must be configured in exactly the same way, and each LDAP host must refer to all additional hosts from which you wish to map groups. For more information about LDAP hosts and referrals, see your LDAP documentation.

To add multiple LDAP Hosts, enter all hosts when you configure LDAP using the LDAP configuration wizard (see [Configuring LDAP authentication](#) for details.) Or if you have already configured LDAP, go to the Authentication management area of the Central Management Console and click the LDAP tab. In the LDAP Server Configuration Summary area, click the name of the LDAP host to open the page that enables you to add or delete hosts.

Note:

- Make sure that you add the primary host first, followed by the remaining failover hosts.
- If you use failover LDAP hosts, you cannot use the highest level of SSL security (that is, you cannot select "Accept server certificate if it comes from a trusted Certificate Authority and the CN attribute of the certificate matches the DNS hostname of the server.") For more information, see [Configuring LDAP authentication](#).

Configuring LDAP Server or Mutual Authentication and the SSL settings

This section describes the CMC related information for configuring SSL with LDAP Server and Mutual Authentication. It assumes that you have completed

the first 10 applicable steps in [Configuring the LDAP host](#), and that you selected either of these for your SSL authentication choice:

- Server Authentication
- Mutual Authentication

You can do this configuration after you complete all the steps in [Configuring the LDAP host](#). For additional information or for information on configuring the LDAP host server, refer to <http://www.techsupport.businessobjects.com/> or your LDAP vendor documentation.

To configure LDAP Server or Mutual Authentication

1. Choose what level of SSL security you want to use from the available options:

Note:

Java applications will ignore the first and last setting and will accept the server certificate only if it comes from a trusted Certificate Authority.

- **Always accept server certificate**

This is the lowest security option. Before BusinessObjects Enterprise 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. BusinessObjects Enterprise 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 BusinessObjects Enterprise 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, BusinessObjects Enterprise must find the Certificate Authority 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 BusinessObjects Enterprise 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, BusinessObjects Enterprise must find the Certificate Authority that issued the certificate in its certificate database. It must also be able to confirm that the CN attribute on the server certificate exactly matches the host name of the LDAP host as you typed it in the "Add LDAP host" field in the first step of the wizard. That is, if you entered the LDAP host name as ABALONE.rd.crystald.net:389, using CN =ABALONE:389 in the certificate would not work.

The host name on the server security certificate is the name of the primary LDAP host. Therefore if you select this option you cannot use a failover LDAP host.

2. In the **SSL host** box, type the host name of each machine, and then click **Add**.

Note:

You must next add the host name of each machine in your BusinessObjects Enterprise system that uses the BusinessObjects Enterprise SDK. (This includes the machine running your Central Management Server and the machine running your WCA.)

3. Specify the SSL settings for each SSL host that has been added to the list, and specify the default settings that will be used for each host that is not on the list.

Note:

The default settings will be used for any setting (for any host) where you leave the "Use default value" box checked or for any machine whose name you do not explicitly add to the list of SSL hosts.

To specify the default settings:

- a. Select default from the SSL list.
- b. Clear the **Use default value** boxes.
- c. Type your values for the "Path to the certificate and key database files" and the "Password for the key database".
- d. If you're specifying settings for Mutual authentication, you can also enter a value in the "Nickname for the client certificate in the cert7.db" field.

To select settings for another host, select its name in the list on the left. Then type the appropriate values in the boxes on the right.

4. Click **Next**.
5. Choose a method of LDAP single sign-on authentication from these choices:
 - Basic (No SSO)
 - SiteMinder

Note:

For further details on configuring SiteMinder, see [Configuring the LDAP plug-in for SiteMinder](#).

6. Choose how new LDAP users and aliases are created.
7. Click **Finish**.

Mapping LDAP groups

Once you have configured LDAP authentication using the LDAP configuration wizard, you can map LDAP groups to Enterprise groups. See [Configuring LDAP authentication](#).

Note:

If you have configured LDAP against AD, this procedure will map your AD groups.

To map LDAP groups using BusinessObjects Enterprise

1. Go to the **Authentication** management area of the CMC.
2. Double-click **LDAP**.

If LDAP authorization 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; click **Add**.

You can add more than one LDAP group by repeating this step. To remove a group, highlight the LDAP group and click Delete.

4. New Alias Options allow you to specify how LDAP aliases are mapped to Enterprise accounts. Select either:
 - **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.

or

- **Create a new account for every added LDAP alias**

Use this option when you want to create a new account for each user.

5. Update Options allow you to specify if LDAP aliases are automatically created for all new users. Select either:

- **New aliases will be added and new users will be created**

Use this option to automatically create a new alias for every LDAP user mapped to BusinessObjects Enterprise. New LDAP accounts are added for users without BusinessObjects Enterprise accounts, or for all users if you selected the "Create a new account for every added LDAP alias" option and clicked **Update**.

or

- **No new aliases will be added and new users will not be created**

Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use BusinessObjects Enterprise. BusinessObjects Enterprise 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 BusinessObjects Enterprise.

6. New User Options allow you to specify properties of the new Enterprise accounts that are created to map to LDAP accounts. Select either:

- **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.

or

- **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 BusinessObjects Enterprise 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 BusinessObjects Enterprise, a 100 user concurrent license could support 250, 500, or 700 users.

7. Click **Update.**

Viewing mapped LDAP users and groups

You can view your LDAP mapped groups in BusinessObjects Enterprise by clicking the LDAP tab (located in the Authentication management area). If LDAP authorization is configured, the Mapped LDAP Member Groups area displays the LDAP groups that have been mapped to BusinessObjects Enterprise.

Unmapping LDAP groups

Similar to mapping, it is possible to unmap groups using BusinessObjects Enterprise.

To unmap LDAP groups using BusinessObjects Enterprise

1. Go to the **Authentication** management area of the CMC.
2. Double-click **LDAP**.

If LDAP authorization 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 BusinessObjects Enterprise.

Tip:

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

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.

Changing LDAP connection parameters and member groups

After you have configured LDAP authentication using the LDAP configuration wizard, you can change LDAP connection parameters and member groups using the LDAP Server Configuration Summary Page.

For information on configuring LDAP authentication using the LDAP configuration wizard, see [Configuring LDAP authentication](#).

To change connection settings

1. Go to the **Authentication** management area of the CMC.
2. Double-click **LDAP**.

If LDAP authorization is configured, the LDAP Server Configuration Summary page appears. On this page you can change any of the connection parameter areas or fields. You can also modify the Mapped LDAP Member Groups area.

3. Delete currently mapped groups that will no longer be accessible under the new connection settings, then click **Update**.
4. Change your connection settings, then click **Update**.
5. Change your Alias and New User options, then click **Update**.
6. Map your new LDAP member groups, then click **Update**.

LDAP and SiteMinder Workflow

To use SiteMinder and LDAP with BusinessObjects Enterprise, you need to make configuration changes in two places:

- In the LDAP plug-in in the CMC.
- In the web.xml file for your web application server.

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 BusinessObjects Enterprise. This section assumes that you have completed [Configuring the LDAP host](#) and chosen SiteMinder for your method of LDAP single sign-on authentication.

Note:

Please 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.

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 the "Single Sign On Type" link 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**. Enter the shared secret again.

Note:

Please 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.

5. Click **Next**.
6. Proceed with configuring the LDAP options.

Modifying web.xml for LDAP and SiteMinder

To enable LDAP and SiteMinder

1. Open the configuration file for InfoView on the machine hosting the web application server.

- For Java application server open the `web.xml` for Java InfoView. This file is located in the following directory:

```
<INSTALLDIR>\Business Objects\BusinessObjects  
Enterprise 12.0\warfiles\WebApps\InfoViewApp\WEB-INF.
```

- For IIS open the NET InfoView `web.config` file. This file is located in the following directory:

```
<INSTALLDIR>\Business Objects\ BusinessObjects  
Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp
```

If you are using the version of Tomcat installed with BusinessObjects Enterprise, the file is located by default in:

```
<Deployed Location>\InfoViewApp\WEB-INF
```

Note:

If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path to substitute.

2. Locate the following string in the file:

```
<param-name>cms.default</param-name>
```

3. Enter the CMS name and port in the `cms.default<param-value>` field. Use the format `servername:portnumber`.

4. Locate the following string in the file:

```
<param-name>authentication.default</param-name>
```

5. Set the `<param-value>` for the `authentication.default` to `secLDAP`.

```
<param-value>secEnterprise</param-value>
```

6. Locate the following string in the file:

```
<param-name>sso.enabled</param-name>
```

7. Change the `<param-value>` for `sso.enabled` from `false` to `true`.

```
<param-value>>true</param-value>
```

8. Locate the following string in the file:

```
<param-name>siteminder.enabled</param-name>
```

9. Change the `<param-value>` for `siteminder.enabled` from `false` to `true`.

```
<param-value>>true</param-value>
```

10. Locate the following string in the file:

```
<param-name>siteminder.authentication</param-name>
```

11. Set the `<param-value>` for `siteminder.authentication` to `secLDAP`.

```
<param-value>secLDAP</param-value>
```

12. Save and close the file.

13. Restart your web application server.

Troubleshooting SiteMinder single sign-on

If you are using SiteMinder with IIS, you may receive an error message in the Central Management Console regarding the failure of single sign-on. If you encounter this message, you may need to manually create two registry keys for SiteMinder:

- Create the following key, set its type to `REG_DWORD`, and set its value to 1:
HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\Enterprise\Admin Plugins\CrystalEnterprise.CMSAdmin\EnableSiteMinderSingleSignOn
- Create a second key, set its type to `REG_SZ`, and set its value to the authentication type that you want to use for SiteMinder single sign-on (`secLDAP` or `secWinAD`):

HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite
12.0\Enterprise\Admin
Plugins\CrystalEnterprise.CMSAdmin\SiteMinderAuthentication

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.

Troubleshooting LDAP accounts

Creating a new LDAP user account

- If you create a new LDAP user account, and the account does not belong to a group account that is mapped to BusinessObjects Enterprise, either map the group to BusinessObjects Enterprise, or add the new LDAP user account to a group that is already mapped to BusinessObjects Enterprise. For more information, see [Configuring LDAP authentication](#).
- If you create a new LDAP user account, and the account belongs to a group account that is mapped to BusinessObjects Enterprise, refresh the user list. For more information, see [Viewing mapped LDAP users and groups](#).

Using AD authentication

This section provides a general description of how Windows Active Directory (AD) authentication works with BusinessObjects Enterprise. It then introduces the administration tools that allow you to manage and configure AD accounts to BusinessObjects Enterprise.

Basic Windows AD authentication workflow

To use AD authentication with BusinessObjects Enterprise 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 BusinessObjects Enterprise applications. This optional step can be facilitated via the following methods:
 - Windows AD with Kerberos
 - Windows AD with NTLM
 - Windows AD with SiteMinder

Support requirements

To facilitate Windows AD authentication on BusinessObjects Enterprise, you should remember the following support requirements.

- The CMS must always be installed on a supported Windows platform.
- Although Windows 2000, 2003 and 2008 are supported platforms for both Kerberos and NTLM authentication, certain BusinessObjects Enterprise applications may only use particular authentication methods. For example, Java applications such as Java InfoView and CMC only support Kerberos, while .NET/COM applications such as .NET InfoView and Import Wizard support both Kerberos and NTLM.

Users from external forests can only authenticate on BusinessObjects Enterprise in the following scenarios:

- Windows 2000: support is only available for NTLM when using .NET/COM applications such as .NET InfoView and Import Wizard) support. For Java applications such as Java InfoView and CMC support is only available for Kerberos.
- Windows 2003 and 2008: Java applications such as Java InfoView and CMC only support Kerberos, while .NET/COM applications such as .NET InfoView and Import Wizard support both Kerberos and NTLM.

Related Topics

- [Mapping AD accounts](#)
- [Using AD authentication with Kerberos](#)
- [Using AD authentication with NTLM](#)
- [Using AD with SiteMinder](#)
- [Windows AD security plug-in](#)
- [Using AD users and groups](#)

Windows AD security plug-in

Windows AD security plug-in enables you to map user accounts and groups from your Microsoft Active Directory (AD) 2000, 2003, and 2008 user database to BusinessObjects Enterprise. It also enables BusinessObjects Enterprise to verify all logon requests that specify Windows AD Authentication. Users are authenticated against the Windows AD user database, and have their membership in a mapped AD group verified before the Central Management Server grants them an active BusinessObjects Enterprise session.

The AD security plug-in enables you to use these authentication methods:

- NTLM
- Kerberos
- SiteMinder

The AD security plug-in is compatible with both Microsoft Active Directory 2000, 2003, and 2008 domains running in either native mode or mixed mode.

Once you have mapped your AD users and groups, all of the BusinessObjects Enterprise client tools support AD authentication. You can also create your own applications that support AD authentication. For more information, see the developer documentation available on the `collaterals` disk of your product distribution.

- AD authentication only works if the CMS is run on Windows. For single sign on to database to work, the reporting servers must also run on Windows. Otherwise all other servers and services can run on all supported platforms.
- The Windows AD plug-in for BusinessObjects Enterprise supports domains within multiple forests.

Using AD users and groups

BusinessObjects Enterprise supports Active Directory (AD) authentication with the Windows security plug-in, which is included by default when the product is installed on Windows. Support for AD authentication means that

users and groups created in Microsoft Active Directory 2000, 2003, and 2008 can be used to authenticate with BusinessObjects Enterprise. This allows you, the administrator, to map previously created user accounts and groups, instead of setting up each user and group within BusinessObjects Enterprise.

Note:

AD authentication only works if the CMS is run on Windows. For single sign on to database to work, the reporting servers must also run on Windows.

The following procedures describe the required steps for setting up Window AD authentication for BusinessObjects Enterprise using either the Kerberos or NTLM protocols.

Mapping AD accounts

To simplify administration, BusinessObjects Enterprise supports Windows AD authentication for user and group accounts. However, before users can use their AD user name and password to log on to BusinessObjects Enterprise, their Windows AD user account needs to be mapped to BusinessObjects Enterprise. When you map an Windows AD account, you can choose to create a new BusinessObjects Enterprise account or link to an existing BusinessObjects Enterprise account.

To map AD users and groups and configure the Windows AD security plug-in

Regardless of which protocol is used, you must complete the following steps to allow AD users to authenticate.

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**.

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 will be populated with the AD Administration names.

5. Enter the name and password of an enabled domain user account. BusinessObjects Enterprise 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)

BusinessObjects Enterprise 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise. Therefore, they will not be able to access BusinessObjects Enterprise.

8. Click **Add**.

The group is added to the list.

You can skip over the configuration of the "Authentication Options", "Synchronization of Credentials" and "SiteMinder Options". For specific information on how to configure Windows AD with Kerberos, NTLM, or SiteMinder see [Using AD authentication with Kerberos](#), [Using AD authentication with NTLM](#), or [Using AD with SiteMinder](#).

9. In the "AD Alias Options" area specify how new aliases are added and updated to BusinessObjects Enterprise.
 - 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 BusinessObjects Enterprise. New AD accounts are added for users without BusinessObjects Enterprise 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 BusinessObjects Enterprise. BusinessObjects Enterprise 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 BusinessObjects Enterprise.

- 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise, a 100 user concurrent license could support 250, 500, or 700 users.

10. 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.

11. 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 BusinessObjects Enterprise.

- **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.

12. You can configure AD group graph updates in the "AD Group Graph Options" area.

- a. Click **Schedule AD Group Graph 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".

13. 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 Group Graph now**

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

Note:

This option affects any scheduled group graph updates. The next scheduled group graph update is listed under "AD Group Graph Options".

- **Update AD Group Graph 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**.

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 Group Graph and Aliases now**

If you click **Update**, neither the group graph nor the user aliases will be updated.

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".

14. Click **Update**.
15. Click **OK**.

Scheduling AD updates

BusinessObjects Enterprise enables administrators to schedule updates for AD group graphs or user aliases. This feature is available for AD authentication with either Kerberos or NTLM. The CMC also enables you to view the time and date when the last update was performed.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will be run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will be 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 be 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 and a start and end date.
Monthly	The update will be 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 and a start and end date.

Recurrence pattern	Description
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 be run on the dates specified in a calendar that has previously been created.

Scheduling group graph updates

BusinessObjects Enterprise relies on Active Directory (AD) for user and group information. To minimize the volume of queries sent to AD, the AD plug-in caches information about groups and how they relate to each other and their user membership. The group graph is recreated every fifteen minutes when no specific schedule is defined.

You can use the CMC to configure the recurrence of the group graph refresh. This should be scheduled to reflect how frequently you will be changing groups and group membership information.

Scheduling AD user alias updates

User objects can be aliased to a Windows Active Directory (AD) account, allowing users to use their AD credentials to log on to BusinessObjects Enterprise. Updates to AD accounts are propagated to BusinessObjects Enterprise by the AD plug-in. Accounts created, deleted, or disabled in AD will be correspondingly created, deleted, or disabled in BusinessObjects Enterprise.

If you do not schedule AD alias updates, updates will only occur when:

- A user logs on: the AD alias will be updated.
- An administrator selects the **Update AD Group Graph and Aliases now** option from the "On-demand AD Update" area of the CMC.

Note:

No AD passwords are stored in the user alias.

Configuring manual AD authentication

Using AD authentication with Kerberos

This section provides information on how to set up BusinessObjects Enterprise to use AD and Kerberos authentication. It includes instructions on setting up service accounts and granting appropriate rights to configure Kerberos with your application server.

- [Configuring Kerberos for your application server](#)
- [General workflow for configuring Kerberos](#)
- [Configuring Kerberos for .NET InfoView and IIS](#)

Configuring Kerberos for your application server

This section contains the tasks related to configuring Kerberos for use with these the following application servers:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- IIS
- SAP NetWeaver 7.10

Tomcat, WebSphere, WebLogic, and Oracle Application Server.

This section contains this information:

- Two type of workflows.
 - The general workflow that you must follow regardless of the web application server you are using.
 - The workflow specific to your web application server. This second workflow is necessary because the implementation of Java Authentication and Authorization Service (JAAS) varies between different application servers.
- The procedural details for each step in the workflow.
- Two samples of Krb5.ini files (for Java application servers).
- Troubleshooting information.

Setting up a service account

To configure BusinessObjects Enterprise 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 BusinessObjects Enterprise servers.

After you set up the service account, you will need to grant the account appropriate rights, see [Granting the service account rights](#).

How you create this account varies slightly depending on what version of Active Directory Domain you are using:

- If you are using a Windows 2000 Domain, see [Setting up a service account on a Windows 2000 Domain](#).
- If you are using a Windows 2003 or 2008 Domain, see [Setting up a service account on a Windows 2003 or 2008 Domain](#).
- If you are using a Windows 2003 or 2008 Domain, you also have the option of setting up constrained delegation. See [Setting up constrained delegation](#) for more information.

Note:

If you are setting up SSO2DB, the service account must be a domain account that has been trusted for delegation.

Note:

In a forest with multiple domains you can create this service account in the domain BusinessObjects Enterprise is installed on. All domains that trust the domain you have created the service account in will be able to authenticate.

Setting up a service account on a Windows 2000 Domain

To set up the service account on a Windows 2000 Domain

1. Create an account on the domain controller or use an existing account.
For detailed instructions, refer to <http://msdn.microsoft.com/>
2. Right-click the user account, then select **Properties**.
3. Click the **Account** tab.
4. Select the **Use DES encryption types for this account** option.

Note:

If you need to set up SSO2DB, you must also select the **Account is trusted for delegation** option.

To run the SPN utility on Windows 2000

1. Download the utility from this location to your Domain controller:

```
http://www.microsoft.com/windows2000/technet/reskit/tools/existing/setspn-o.asp
```

Note:

The SETSPN utility is a program that allows you to manage the Service Principal Name (SPN) for service accounts in Active Directory.

2. Open a command prompt and enter this command:

```
SETSPN.exe -A <ServiceClass>/<DomainName> <Serviceaccount>
```

Replace *<ServiceClass>* with any desired name. For example, BOBJCentralMS. (For clustered CMSs, use a generic name; do not use the host name of a CMS machine.) Replace *<DomainName>* with the domain name of the service account. For example, domain.com. Replace *<ServiceAccount>* with the domain user account that you've configured.

Note:

- The name of your service account is case-sensitive.
- The SPN must be unique in the forest in which it is registered. One way to check is to use Windows support tool `Ldp.exe` to search for the SPN.

3. Verify that you receive a message similar to this one:

```
Registering ServicePrincipalNames for CN=ServiceCMS,CN=Users,DC=DOMAIN,DC=COM BOBJCentralMS/domain.com Updated object
```

Setting up a service account on a Windows 2003 or 2008 Domain
To set up the service account on a Windows 2003 or 2008 Domain

Note:

With a Windows 2003 or 2008 Domain, RC4 is the default encryption type and should be used. You will need BusinessObjects Enterprise to be running with JDK 1.5 or higher. (It ships with BusinessObjects Enterprise and is installed by default.) If you want to use a lower JDK, you must check "Use DES encryption".

Note:

If you are using WebLogic 9.2 (which does not work with RC4), you must check "Use DES encryption". You also need the WebLogic's MP2 patch for WebLogic 9.2.

1. Create a new account on the domain controller or use an existing account.

For detailed instructions, refer to <http://msdn.microsoft.com/>

2. Open a command prompt and enter this command:

```
SETSPN.exe -A <ServiceClass>/<DomainName> <Serviceaccount>
```

Replace *<ServiceClass>* with any desired name. For example, BOBJ CentralMS. (For clustered CMSs, use a generic name; do not use the host name of a CMS machine.) Replace *<DomainName>* with the domain name of the service account. For example, domain.com. Replace *<ServiceAccount>* with the domain user account that you've configured.

Note:

- The name of your service account is case-sensitive.
- The SPN must be unique in the forest in which it is registered. One way to check is to use Windows support tool `Ldp.exe` to search for the SPN.

3. Verify that you receive a message similar to this one:

```
Registering ServicePrincipalNames for  
CN=ServiceCMS,CN=Users,DC=DOMAIN,DC=COM  
BOBJCentralMS/domain.com Updated object
```

4. If you are using SSO2DB, open the account properties, click the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**.

Note:

You will not see the Delegation tab until after you have entered the SETSPN command.

5. Click **OK**.

Setting up constrained delegation

If your company has a policy against trusting a specific service account for delegation to any service, and you are using Active Directory on Windows 2003 or 2008, you may set up constrained delegation. Setting up constrained delegation is done after you create the service account. Constrained delegation allows you to limit what services an account or computer can delegate to, rather than allowing an authorized user to delegate to all services. You can set up constrained delegation for Java applications by using a service account.

This method allows you to limit the amount of delegation permitted. Constrained delegation for a service account allows you to do further limit delegation to a specific service for a specific user on a specific computer. Because constrained delegation for a service account is more restrictive, it is considered a more secure option.

Note:

- Constrained delegation is supported only on Active Directory 2003 and 2008.
- The account needs to be trusted for delegation only if you plan to use SSO2DB.

To set up constrained delegation for a service account

1. Create an SPN for the CMS server.

Type the following command:

```
SETSPN.exe -A <ServiceClass>/<DomainName> <Serviceaccount>
```

- Replace `<ServiceClass>` with any desired name. For example, BOBJCentralMS. For clustered CMSs do not use the hostname of a CMS machine; use a generic name.
- Replace `<DomainName>` with the domain name of the service account. For example, domain.com.
- Replace `<ServiceAccount>` with the name of the service account you just created.

2. Open Active Directory Users and Computers.

3. Select the Users folder.

4. Select the service account user.

5. Right-click, then select Properties.

6. Click the Delegation tab.

7. Select Trust this user for delegation to specified services only.

8. Ensure Use Kerberos only is selected.

9. Click Add.

10. Click Users and Computers.

11. Enter the `<ServiceAccount>` you specified in step 2, then click OK.

12. Select the `<ServiceClass>` name that you've chosen from the list of services, then click OK.

13. Click OK.

Configuring the servers

Configuring the BusinessObjects Enterprise servers includes these steps:

- [Granting the service account rights](#)
- [Adding the Service Account to the servers' Local Administrators group](#)
- [Configuring the servers to use the service account](#)

Granting the service account rights

In order to support AD and Kerberos, you must grant the service account the right to act as part of the operating system. This must be done on each machine running a Server Intelligence Agent (SIA) with the following servers:

- CMS

- Crystal Reports Processing Server (required only for SSO2DB)
- Report Application Server (required only for SSO2DB)
- Web Intelligence Processing Server (required only for SSO2DB)

Note:

If you're using SSO2DB, you require a service account that has been trusted for delegation. See [Setting up a service account](#).

To grant the service account rights

1. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Expand **Local Policies**, then click **User Rights Assignment**.
3. Double-click **Act as part of the operating system**.
4. Click **Add**.
5. Enter the name of the service account you created, then click **OK**.
6. Ensure that the **Local Policy Setting** check box is selected, and click **OK**.
7. Repeat the above steps on each machine running a BusinessObjects Enterprise server.

Note:

It is important that the Effective Right ends up being checked after **Act as part of the operating system** is selected. Typically, you will need to restart the server for this to occur. If, after restarting the server, this option is still not on, your Local Policy settings are being overridden by your Domain Policy settings.

Adding the Service Account to the servers' Local Administrators group

In order to support Kerberos, the service account must be part of the local Administrators group for each server that has a SIA with one of the following services deployed:

- CMS
- Crystal Reports Processing Server (required only for SSO2DB)
- Report Application Server (required only for SSO2DB)
- Web Intelligence Processing Server (required only for SSO2DB)

Note:

If you're using SSO2DB, you require a service account that has been trusted for delegation. See [Setting up a service account](#). You must also have administrative rights on the server.

To add an account to the Administrator's group

1. On the desired machine, right-click **My Computer** and click **Manage**.
2. Go to **System Tools > Local Users and Groups > Groups**.
3. Right-click **Administrators**, then click **Add to Group**.
4. Click **Add** and type the logon name of the service account.
5. Click **Check Names** to ensure that the account resolves.
6. Click **OK**, then click **OK** again.
7. Repeat these steps for each Business Objects server that has to be configured.

Configuring the servers to use the service account

To support Kerberos single sign-on, you must configure the SIA that contains the following servers to log on as the service account:

- CMS server
- Crystal Reports Processing Server (required only for SSO2DB)
- Report Application Server (required only for SSO2DB)
- Web Intelligence Processing Server (required only for SSO2DB)

Note:

If you're using SSO2DB, you require a service account that has been trusted for delegation. See [Setting up a service account](#).

*To configure a server***Note:**

You need to perform the following steps for any Server Intelligence Agent that is running services used in the previous steps for configuring the service account.

1. In the Central Configuration Manager (CCM), stop the Server Intelligence Agent (SIA).

Note:

When you stop the SIA, all services managed by the SIA are stopped.

2. Double-click the SIA to view its properties.
3. On the Properties tab, in the Log On As area, deselect the **System Account** check box.
4. Provide the user name and password for the service account you created earlier, click **Apply**, then click **OK**.

Note:

For information about creating the service account, see [Setting up a service account](#).

5. Restart the SIA.
6. If necessary, repeat steps 1 through 5 for each SIA that is running a service that has to be configured.

General workflow for configuring Kerberos

This section outlines the process of setting up BusinessObjects Enterprise to use AD with Kerberos authentication.

Setting up Kerberos includes these steps:

- [Setting up a service account](#)
- [Granting the service account rights](#)
- [Configuring the servers to use the service account](#)
- [Enabling Kerberos authentication in the Windows AD plug-in](#)

Workflow for configuring Tomcat for Kerberos

If you are using Tomcat, and you want to use Kerberos, you must complete these steps, in addition to the [General workflow for configuring Kerberos](#).

- [To create the Kerberos configuration file for Tomcat, WebLogic or Oracle Application Server](#)
- [To create the JAAS login configuration file for Tomcat or WebLogic](#)
- [To modify the Java options for Kerberos on Tomcat](#)

Workflow for configuring WebSphere for Kerberos

If you are using WebSphere, and you want to use Kerberos, you must complete these steps, in addition to the [General workflow for configuring Kerberos](#).

- [Configuring Kerberos and single sign-on for Java InfoView](#)
- [To create the JAAS login configuration file for WebSphere](#)
- [To modify the Java options for Kerberos on WebSphere](#)

Workflow for configuring WebLogic for Kerberos

If you are using WebLogic, and you want to use Kerberos, you must complete these steps, in addition to the [General workflow for configuring Kerberos](#).

- [To create the Kerberos configuration file for Tomcat, WebLogic or Oracle Application Server](#)
- [To create the JAAS login configuration file for Tomcat or WebLogic](#)
- [To modify the Java options for Kerberos on WebLogic](#)

Workflow for configuring Oracle for Kerberos

If you are using Oracle, and you want to use Kerberos, you must complete these steps, in addition to the [General workflow for configuring Kerberos](#).

- [To create the Kerberos configuration file for Tomcat, WebLogic or Oracle Application Server](#)
- [To create the JAAS login configuration file for Oracle Application Server](#)
- [To modify the Java options for Kerberos on Oracle Application Server](#)

Workflow for configuring IIS for Kerberos

Configuring AD and Kerberos for .NET InfoView includes these steps:

- [Setting up a service account](#)
- [Configuring the servers](#)
- [Configuring Kerberos for .NET InfoView and IIS](#)

Enabling Kerberos authentication in the Windows AD plug-in

In order to support Kerberos, you have to configure the Windows AD security plug-in in the CMC to use Kerberos authentication. This includes:

- Ensuring Windows AD authentication is enabled.
- Entering the AD Administrator account.

Note:

This account requires read access to Active Directory only; it does not require any other rights.

- Enabling Kerberos authentication and single sign-on, if single sign-on is desired.

Note:

If you enable single sign-on in the CMC, you also must configure it in the `web.xml` or `web.config` file for InfoView.

- Entering the service principal name (SPN) for the service account.

Related Topics

- [Configuring Kerberos and single sign-on for Java InfoView](#)
- [Configuring Kerberos and single sign-on for .NET InfoView](#)

Prerequisites

Before you configure the Windows AD security plug-in for Kerberos, you must have completed the following tasks:

- [Setting up a service account](#)
- [Granting the service account rights](#)
- [Configuring the servers to use the service account](#)
- [Mapping AD accounts](#)

To configure the Windows AD security plug-in for Kerberos

You should review the steps outlined in the following section: [To map AD users and groups and configure the Windows AD security plug-in](#)

1. Go to the **Authentication** management area of the CMC.
2. Double-click **Windows AD**.
3. Ensure that the **Windows Active Directory Authentication is enabled** check box is selected.
4. Under **Authentication Options**, select **Use Kerberos authentication**.
5. If you want to configure single sign-on to a database, select the **Cache Security context** (required for SSO to database) check box.
6. In the **Service principal name** field, enter the SPN mapped to the service account.

Note:

When manually logging on to Java InfoView, users from other domains must append the domain name in upper case after their user name. For example: user@CHILD.PARENTDOMAIN.COM.

7. If you want to configure single sign-on, select **Enable Single Sign On for selected authentication mode**.

Note:

If you selected to enable single sign on, you will need to configure either the InfoView `web.xml` or the `web.config` file.

Related Topics

- [Single sign-on with Windows AD](#)

Configuring Kerberos for your Java application server

The specific process of configuring Kerberos for a Java application server varies slightly depending on which Java application server is used. However, the general process of configuring Kerberos on your application server involves these steps:

- Creating the Kerberos configuration file.
- Creating the JAAS login configuration file.
- Modifying the Java Options.
- Restarting your Java application server.

Note:

- The default Active Directory domain must be in uppercase DNS format.
- You don't need to download and install MIT Kerberos for Windows. You also no longer require a key tab for your service account.
- If you are using Vintela SSO you do not need the `krb.ini` or `bsclogin.conf` files.

To create the Kerberos configuration file for Tomcat, WebLogic or Oracle Application Server

Follow these steps to create the Kerberos configuration file if you're using Tomcat, Oracle Application Server or WebLogic.

1. Create the file `krb5.ini`, if it does not exist, and store it under C:\WINNT for Windows.

Note:

- If the application server is installed on UNIX, you should use the following directories:

Solaris: /etc/krb5/krb5.conf

Linux: /etc/krb5.conf

- You can store this file in a different location, however if you do, you will need to specify its location in your java options. See [Modifying your Java options for Kerberos](#). For more information on `krb5.ini` go to <http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view>.

2. Add the following required information in the Kerberos configuration file:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

Note:

- `DNS.COM` is the DNS name of your domain which must be entered in uppercase in FQDN format.
- `kdc` is the Host name of the Domain Controller.

- You can add multiple domain entries to the [realms] section if your users log in from multiple domains. To see a sample of this file with multiple domain entries, see [Sample Krb5.ini files](#).
- In a multiple domain configuration, under [libdefaults] the default_realm value may be any of the desired domains. The best practice is to use the domain with the greatest number of users that will be authenticating with their AD accounts. If no UPN suffix is supplied during at log on, it defaults to the value of default_realm. This value should be consistent with **default domain** setting in CMC.

To create the Kerberos configuration file for WebSphere

1. Create the file `krb5.ini`, if it does not exist, and store it under `C:\WINNT` for Windows.

Note:

- You can store this file in a different location, however if you do, you will need to specify its location in your java options. See [Modifying your Java options for Kerberos](#).
 - To see sample `krb5.ini` files, see [Sample Krb5.ini files](#).
2. Add the following required information in the Kerberos configuration file:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
```

```
DOMAIN.COM =  
}
```

Note:

- If you are using DES encryption, change `rc4-hmac` to `des-cbc-crc`.
- `DOMAIN.COM` is the DNS name of your domain which must be entered in uppercase in FQDN format.
- `hostname` is the Host name of the Domain Controller.
- `[capath]` defines the trust between domains that are in another AD forest. In the example above `DOMAIN2.COM` is a domain in an external forest and has direct two way transitive trust to `DOMAIN.COM`.

3. Save and close the file.

To create the JAAS login configuration file for Tomcat or WebLogic

1. Create a file called `bscLogin.conf` if it does not exist, and store it in the default location: `C:\WINNT`.

Note:

You can store this file in a different location. However, if you do, you will need to specify its location in your java options. See [Modifying your Java options for Kerberos](#).

2. Add the following code to your JAAS `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {  
com.sun.security.auth.module.Krb5LoginModule required;  
};
```

3. Save and close the file.

To create the JAAS login configuration file for Oracle Application Server

1. Locate the `jazn-data.xml` file.

Note:

This default location for this file is `C:\OraHome_1\j2ee\home\config`. If you installed Oracle Application Server in a different location, find the file specific to your installation.

2. Add the following content to the file between the `<jazn-loginconfig>` tags:

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Save and close the file.

To create the JAAS login configuration file for WebSphere

1. Create a file called `bscLogin.conf` if it does not exist, and store it in the default location: `C:\WINNT`
2. Add the following code to your JAAS `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Save and close the file.

Sample Krb5.ini files

Sample multiple domain Krb5.ini file

The following is a sample file with multiple domains:

```
[domain_realm]
; trust relationship: childtest4<->bobjtest3<->bob
jtest<->bobjtest2
[libdefaults]
default_realm = BOBJTEST.COM
[realms]
BOBJTEST.COM = {
kdc = VANPGVMBOBJ01.bobjtest.com
}
BOBJTEST2.COM = {
kdc = VANPGVMBOBJ05.bobjtest2.com
```

```
}  
BOBJTEST3.COM = {  
    kdc = VANPGVMBOBJ07.bobjtest3.com  
}  
CHILDTEST4.BOBJTEST3.COM = {  
    kdc = vanpgvmbobj08.childtest4.bobjtest3.com  
}  
[capaths]  
; for clients in bobjtest3 to login bobjtest2  
BOBJTEST3.COM = {  
    BOBJTEST2.COM = BOBJTEST.COM  
}  
; for clients in childtest4 to login bobjtest2  
CHILDTEST4.BOBJTEST3.COM = {  
    BOBJTEST2.COM = BOBJTEST.COM  
    BOBJTEST2.COM = BOBJTEST3.COM  
}
```

Sample single domain Krb5.ini file

Following is a sample krb5.ini file with a single domain.

```
[realms]  
BOBJTEST2.COM = {  
    kdc = VANPGVMBOBJ05.bobjtest2.com  
}
```

Modifying your Java options for Kerberos

You need to configure specific Java options depending on the application server you are using:

- [To modify the Java options for Kerberos on Tomcat](#)
- [To modify the Java options for Kerberos on WebLogic](#)
- [To modify the Java options for Kerberos on Oracle Application Server](#)
- [To modify the Java options for Kerberos on WebSphere](#)

To modify the Java options for Kerberos on Tomcat

1. From the **Start** menu, select **Programs > Tomcat > Tomcat Configuration**.
2. Click the **Java** tab.

3. Add the following options:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf  
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

Replace XXXX with the location you stored the file.

4. Close the Tomcat configuration file.

5. Restart Tomcat.

To modify the Java options for Kerberos on WebLogic

If you are using Kerberos with WebLogic, your Java options need to be modified to specify the location of the Kerberos configuration file and the Kerberos login module.

1. Stop the domain of WebLogic that runs your BusinessObjects Enterprise applications.
2. Open the script that starts the domain of WebLogic that runs your BusinessObjects Enterprise applications (`startWeblogic.cmd` for Windows, `startWebLogic.sh` for UNIX).
3. Add the following information to the `Java_Options` section of the file:

```
set JAVA_OPTIONS=-Djava.security.auth.login.con  
fig=C:/XXXX/bscLogin.conf -Djava.securi  
ty.krb5.conf=C:/XXX/krb5.ini
```

Replace XXXX with the location you stored the file.

4. Restart the domain of WebLogic that runs your BusinessObjects Enterprise applications.

To modify the Java options for Kerberos on Oracle Application Server

If you are using Kerberos with Oracle Application Server, the Java options need to be modified to specify the location of the Kerberos configuration file.

1. Log on to the administration console of your Oracle Application Server.
2. Click the name of the OC4J instance that runs your BusinessObjects Enterprise applications.
3. Select Server Properties.
4. Scroll down to the Multiple VM Configuration section.
5. In the Command Line Options section, append the following at the end of the Java Options text field: `-Djava.securi`

`ty.krb5.conf=C:/XXXX/krb5.ini` replacing XXXX with the location where you stored the file.

6. Restart your OC4J instance.

To modify the Java options for Kerberos on WebSphere

1. Log into the administrative console for WebSphere.

For IBM WebSphere 5.1, type `http://servername:9090/admin`. For IBM WebSphere 6.0, type `http://servername:9060/ibm/console`

2. Expand Server, click Application Servers, and then click the name of the application server you created to use with BusinessObjects Enterprise.
3. Go to the JVM page.

If you are using WebSphere 5.1, follow these steps to get to the JVM page.

- a. On the server page, scroll down until you see **Process Definition** in the **Additional Properties** column.
- b. Click **Process Definition**.
- c. Scroll down and click **Java Virtual Machine**.

If you are using WebSphere 6.0, follow these steps to get to the JVM page.

- a. On the server page, select **Java and Process Management**.
 - b. Select **Process Definition**.
 - c. Select **Java Virtual Machine**.
4. Click **Generic JVM arguments** then type the location of your Krb5.ini and the location of your bscLogin.conf file.

`-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf`

`-Djava.security.krb5.conf=C:\XXXX\krb5.ini`

Replace XXXX with the location you stored the file.

5. Click **Apply**, and then click **Save**.
6. Stop and restart the server.

Configuring Kerberos and Vintela Single Sign-On with SAP NetWeaver 7.10

To use Kerberos and Vintela single sign-on with SAP NetWeaver 7.10, configure the system as if you were using the Tomcat web application server. You will not need to create a bscLogin.conf file.

Once this has been done, you will need to add a LoginModule and update some Java settings on SAP NetWeaver 7.10.

To configure NetWeaver security

In order to correctly map the com.sun.security.auth.module.Krb5LoginModule to the com.businessobjects.security.jgss.initiate we need to manually add a LoginModule to Netweaver.

1. Open the NetWeaver Administrator by typing the following address into a web browser: `http://<machine name>:<port>/nwa`.
2. Click **Configuration Management > Security > Authentication > Login Modules > Edit**.
3. Add a new login module with the following information.

Display Name	Krb5LoginModule
Class Name	com.sun.security.auth.module.Krb5LoginModule

4. Click **Save**.
NetWeaver creates the new module.
5. Click **Components > Edit**
6. Add a new Policy called com.businessobjects.security.jgss.initiate.
7. In the Authentication Stack, add the login module we created in Step 3, and set it to **Required**.
8. Confirm that there are no other entries in the "Options for Selected Login Module". If there are, remove them.
9. Click **Save**.
10. Log out of the NetWeaver Administrator.

To configure Java options for NetWeaver

1. Browse to the Java configuration tool (located at `C:\usr\sap\<NetWeaver ID>\<instance>\j2ee\configtool\` by default) and double-click `configtool.bat`.
The configuration tool opens.
2. Click **View > Expert Mode**.
3. Expand **Cluster-Data > Template**.
4. Select the Instance that corresponds to your NetWeaver server (for example **Instance - <system ID><machine name>**).
5. Click **VM Parameters**.
6. Select **SAP** from the **Vendor** drop down, and **GLOBAL** from the **Platform** drop down.
7. Click **System**.
8. Add the following custom parameter information:

java.security.krb5.conf	<path to the krb5.ini file including the file name>
javax.security.auth.useSubjectCredsOnly	false

9. Click **Save**.
10. Click **Configuration Editor**.
11. Click **Configurations > Security > Configurations > com.businessobjects.security.jgss.initiate > Security > Authentication**.
12. Click **Edit Mode**.
13. Right-click on the **Authentication** node and select **Create sub-node**.
14. Select **Value-Entry** from the top drop-down.
15. Enter the following:

Name	create_security_session
Value	false

16. Click **Create**.
17. Close the Window.

18. Click **Config Tool**.

19. Click **Save**.

Once you have updated your configuration, you will need to restart your NetWeaver server.

Configuring Kerberos for .NET InfoView and IIS

Additional configuration steps are required for authentication to BusinessObjects Enterprise .NET InfoView with Windows AD. Once these steps have been implemented, users will be able to enter their AD username and password to logon to .NET InfoView via Kerberos authentication.

Note:

If you wish to allow users to logon to Java Applications as well, please see the section on Configuring Kerberos for your Java Applications server.

To configure Kerberos for .NET InfoView and IIS

The steps below must be implemented after you have performed all of the following:

- Mapped AD users and groups
- Configured the Windows AD security plug-in for Kerberos authentication
- Set up a service account
- Configured Kerberos for you application server

1. Open the `web.config` file for .NET InfoView.

The file is by default installed in the following directory:<INSTALLDIR>
\Business Objects\BusinessObjects Enterprise 12.0\Web
Content\InfoViewApp\InfoViewApp\.

2. Modify the `web.config` file settings:

- To set Windows AD as default authentication option for InfoView, modify the `<add key="authentication.default" value="secEnterprise"/>` section to `<add key="authentication.default" value="secWinAD"/>`
- If you want the user to select an authentication option before logging on to InfoView, modify the `<add key="authentication.visible" value="false"/>` section to `<add key="authentication.visible" value="true"/>`.

3. Save and close the `web.config` file.

4. Restart IIS.

Users will now be able to use their AD usernames and passwords to logon to .NET InfoView via Kerberos authentication.

Users should now be able to logon to .NET InfoView with their AD username and password via Kerberos authentication.

Note:

Users in the same forest will need to logon with either `DOMAIN\username` or `username@DOMAIN.COM`. Users in External Forests will need to logon with `username@DOMAIN.COM`.

Related Topics

- [To map AD users and groups and configure the Windows AD security plug-in](#)
- [Setting up a service account](#)
- [Configuring the servers](#)

Server cache expiry

When the system is using AD and Kerberos single sign-on, it uses the cache expiry for certain BusinessObjects Enterprise servers to determine whether a logon ticket is still valid. This applies to the CMS, Crystal Reports Processing Server, Report Application Server, and Web Intelligence Processing Server.

The CMS uses the cache expiry as follows:

- If the CMS cache expiry is greater than that of the ticket, the system renews the ticket until the CMS cache expiry is reached.
- If the CMS cache expiry is less than that of the ticket, the ticket will expire when the CMS cache expiry is reached.
- If the CMS cache expiry is zero, the system will use the globally set ticket expiry.

The other servers use either their cache expiry or the ticket expiry, whichever has the lowest value. Regardless of whether the cache expiry for the server is greater or less than that of the ticket, the ticket will expire when the lowest expiry value is reached.

The system comes configured with default values for the server cache expiry. To change the default values for the cache expiry, see [Modifying the default cache expiry value](#).

Note:

If you are running multiple instances of a server, you can control the cache expiry for each instance individually.

Modifying the default cache expiry value

To change the default cache expiry value

1. Go to the **Servers** management area of the CMC.
2. Click the link for the server.
3. Choose **Properties** from the **Manage** menu.
4. Change the **Single Sign-On Expiry** value, then click **Save**.

Troubleshooting Kerberos

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Java SDK Kerberos configuration

To enable logging

1. From the **Start** menu, select **Programs > Tomcat > Tomcat Configuration**
2. Click the **Java** tab.
3. Add the following options:

```
-Dcrystal.enterprise.trace.configuration=verbose  
-sun.security.krb5.debug=true
```

This will create a log file in the following location:

```
C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
```

To test your Java Kerberos configuration

- Run the following command to test your Kerberos configuration, where `servact` is the service account and domain under which the CMS is

running, and `password` is the password associated with the service account.

```
<Install Directory>\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

For example:

```
C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

If you still have a problem, ensure that the case you entered for your domain and service principal name match exactly with what is set in Active Directory.

Mapped AD user unable to log on to CMC or InfoView

The following two issues may occur, despite the fact that the users have been mapped to BusinessObjects Enterprise:

- [Logon failure due to different AD UPN and SAM names](#)
- [Pre-authentication error](#)

Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to BusinessObjects Enterprise. Despite this fact, they are unable to successfully log on to CMC or InfoView with Java AD authentication and Kerberos in the following format: `DOMAIN\ABC123`

This problem can happen when the user is set up in Active Directory with a UPN and SAM name that are not the same, either in case or otherwise. Following are two examples which may cause a problem:

- The UPN is `abc123@company.com` but the SAM name is `DOMAIN\ABC123`.
- The UPN is `jsmith@company` but the SAM name is `DOMAIN\johnsmith`.

There are two ways to address this problem:

- Have users log in using the UPN name rather than the SAM name.
- Ensure the SAM account name and the UPN name are the same.

Pre-authentication error

A user who has previously been able to log on, can no longer log on successfully. The user will receive this error: Account Information Not Recognized. The Tomcat error logs reveal the following error: "Pre-authentication information was invalid (24) "

This can occur because the Kerberos user database didn't get a change made to UPN in AD. This may mean that the Kerberos user database and the AD information are out of sync.

To resolve this problem, reset the user's password in AD. This will ensure the changes are propagated correctly.

Note:

This problem is not an issue with J2SE 5.0.

Using AD authentication with NTLM

This section provides information on how to setup manual NTLM authentication to BusinessObjects Enterprise .NET InfoView with Windows AD. Once these steps have been implemented, users will be able to enter their AD username and password to logon to .NET InfoView as well as other BusinessObjects Enterprise Windows applications

Note:

With NTLM Authentication, users can use their AD credentials to authenticate to .NET InfoView, .NET Applications, and Windows BusinessObjects Enterprise thick client applications such as Crystal Reports or Import Wizard. However users will not be able to use their AD credentials to authenticate to Java applications such Central Management Console (CMC) and Web Services. If your users need to authenticate to both .NET and Java applications, you must use Kerberos authentication.

Configuring AD single sign on

Single sign-on with Windows AD

The Windows AD security plug-in supports single sign-on, thereby allowing authenticated AD users to log on to BusinessObjects Enterprise without explicitly entering their credentials. The single sign-on requirements depend upon the way in which users access BusinessObjects Enterprise: either via a thick client, or over the Web. In both scenarios, the security plug-in obtains the security context for the user from the authentication provider, and grants the user an active BusinessObjects Enterprise session if the user is a member of a mapped AD group.

To obtain AD single sign-on functionality from a thick-client application (such as the Publishing Wizard), the user must be running a Windows operating system, and the application must use the BusinessObjects Enterprise SDK. In this scenario, the Windows AD security plug-in queries the operating system for the current user's credentials when the client is launched.

Configuring Kerberos and single sign-on for Java InfoView

The following procedure explains how to enable Kerberos single sign-on for Java InfoView.

Note:

If you plan to use single sign-on to Java InfoView in a reverse proxy environment, read [Configuring reverse proxy servers for BusinessObjects Enterprise web applications](#) before proceeding.

Before you configure single sign-on for Java InfoView, you must complete configuration prerequisites: these prerequisites are the steps from the [General workflow for configuring Kerberos](#) and the steps that apply specifically to your type of Java application server.

Also, ensure that single sign-on is enabled in the Authentication settings in the CMC. For details, go to [Enabling Kerberos authentication in the Windows AD plug-in](#).

See these sections for the configuration steps that apply specifically to your Java application server:

- [Workflow for configuring Tomcat for Kerberos](#)
- [Workflow for configuring WebSphere for Kerberos](#)
- [Workflow for configuring WebLogic for Kerberos](#)
- [Workflow for configuring Oracle for Kerberos](#)

Workflow for configuring Kerberos single sign-on to Java InfoView

To configure Kerberos single sign-on for Java InfoView, complete the six steps in the following table.

Step 1	<i>To create a service account with delegation to be used for Vintela single sign-on for Java</i>
Step 2	<i>To create an SPN for your web application server</i>
Step 3	<i>To reset the service account password</i>
Step 4	<i>To create and place a keytab file</i>
Step 5	<i>To enable Vintela single sign-on for Java in the web.xml file</i>
Step 6	<i>Setting up multiple SPNs</i>
Step 7	<i>To increase the header size limit of your Java application server</i>

The following sections describe how to complete each of these steps.

In addition to the steps you must complete, you may also want to change either of these configurable items available with Vintela single sign-on for Java:

- The level of error logging recorded.
- The text users receive if their authentication with Vintela single sign-on for Java fails.

For details, see [Modifying the Vintela logon error page](#) and [Controlling logging with Vintela single sign-on for Java](#).

The final section, [Alternate URL to access InfoView](#), explains why there is an alternate page provided and lists the URL for this page.

To create a service account with delegation to be used for Vintela single sign-on for Java

To set up user authentication for a service, you must register the service as a user in AD on the Domain Controller.

1. To register the service, on the Domain Controller, open the Active Directory Users and Computers snap in.
2. Click the Users folder to display a list of users and on the Action menu, click **New** and then click **User**.
3. Enter a name and logon name for the new service, and then click **Next**.
4. On the next screen, enter a password for the service.

Ensure that the **User must change password at next logon** option is not selected.

5. Click **Next** and then click **Finish**.
6. Right-click the user you have entered in the User folder list, and then click **Properties**.
7. Click the Account tab and then select **Account is trusted for delegation** and **Password never expires**.

This prevents the service account from expiring, which would cause Kerberos errors.

Note:

- If AD is deployed in a Windows 2003 Domain, the Account is trusted for delegation option is not available until a Service Principal Name has been created and mapped to this account. If you do not see this

option, complete the steps in the next section, then open the user account in the AD Users and Computers snap in and select the Delegation tab.

- This service account cannot currently be set up with Microsoft's constrained delegation.
8. If your Domain Controller is running in a lower Domain Functional Level (lower than Windows 2003 Domain), view the Account properties for the user you created in step 2, and select **Use DES encryption types for this account**.

Note:

In Windows 2003 and 2008, Domain Functional Level RC4 is used by default.

9. Click **OK**.

To create an SPN for your web application server

Note:

Make sure that the SPN you are creating does not already exist and is mapped to another account. If so, you must remove this SPN with the setspn utility or delete the account that the SPN is mapping to.

1. Launch a command prompt and navigate to your Support Tools folder.
2. Execute the following command:

```
ktpass -princ HTTP/<myurl>@<REALM> -mapuser <user>
```

where

- <myurl> is the URL that your users type in their web browser to access InfoView. For example, if the URL is http://examplemachine.exampledomain.com:8080/InfoViewApp/ then <myurl> must be: examplemachine.exampledomain.com.
- <REALM> is the Active Directory realm in which the server is located. (For example, EXAMPLE.COM).
- <user> is the logon name of the user account you created above.

To reset the service account password

To prevent Kerberos integrity-check failures, you should reset the password of the user account you created in step 1.

1. On the Domain Controller with Active Directory installed, on the **Start** menu click **Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the user account you created previously and click **Reset Password**.
3. Enter and confirm the same password that you entered previously.
4. Ensure that **User must change password at next logon** is not selected and click **OK**.

To create and place a keytab file

You can configure the Kerberos filter to use either a password or a keytab file. A keytab file is the recommended method because it is more secure. A keytab file allows the Kerberos filter to be configured without exposing the password of the user account on the web application machine.

1. Run `ktpass` with the following arguments at command prompt:

```
ktpass -out keytab_filename -princ HTTP/host@REALM -
pass user_password -kvno 255
-ptype KRB5_NT_PRINCIPAL -crypto encryption_type
```

where

- `keytab_filename` is the name of the keytab file we want to generate. (host.keytab, for example).
 - `HTTP/host@REALM` is the SPN created in [To create an SPN for your web application server](#) (for example, `HTTP/myurl.mydomain.com@MYDOMAIN.COM`).
 - `user_password` is the password of the user used in the Map a Service Principle Name (SPN) section.
 - `encryption_type` is the type of encryption associated with the service account you created in [To create a service account with delegation to be used for Vintela single sign-on for Java](#). If you are using DES encryption, use `DES-CBC-MD5`. If you are using RC4 encryption, use `RC4-HMAC-NT`.
2. Copy the generated keytab file onto the java application machine and place in your chosen location.

Note:

- The keytab is usually found in the same folder as your `ktpass` support tool unless you specified a different location.

- Typically the keytab is stored in C:/WINNT or C:/Windows.

To enable Vintela single sign-on for Java in the web.xml file

This procedure can be used for both InfoView and OpenDocument.

Note:

If you are using WebLogic as your application server, read [Special considerations for WebLogic](#) before proceeding.

1. Open the `web.xml` file for InfoView or OpenDocument from its deployed location on your web application server.

The InfoView `web.xml` file is stored in the following location on Windows:

```
<INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\warfiles\WebApps\InfoViewApp\WEB-INF.
```

The OpenDocument `web.xml` file is stored here: `<INSTALLDIR>\Business Objects\BusinessObjects Enterprise`

```
12.0\warfiles\WebApps\OpenDocument\WEB-INF.
```

Note:

- If you are using the version of Tomcat installed with BusinessObjects Enterprise on Windows, and you did not modify the default installation location, replace `<INSTALLDIR>` with `C:\Program Files`
 - If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path.
2. Find the following parameters and make the appropriate changes:

<param-name>	Original <param-value>	New <param-value>
cms.default (for the InfoView web.xml file only)	your CMS name and port number	your CMS name and port number
opendoc.cms.default (for the OpenDocument web.xml file only)	default CMS	default CMS

<param-name>	Original <param-value>	New <param-value>
authentication.default	SecEnterprise	SecWinAD
siteminder.enabled	true	false
vintela.enabled	false	true
sso.enabled	false	false

- Find the following section in the web.xml file:

```
<!-- For Vintela SSO the following filter needs to be
uncommented.
There is also a filter mapping which needs to be uncom
mented.
Set idm.realm to the Active Directory realm where the
server is in
and idm.princ to the service principal name.
-->
```

- Remove the comment start tag that immediately follows this comment as well as its corresponding end tag.
- Find the following section in the web.xml file:

```
<!-- For Vintela SSO the following filter mappings
need to be uncommented.
There is also a filter which needs to be uncom
mented.
-->
```

- Remove the comment start tag that immediately follows this comment as well as its corresponding end tag.
- For the OpenDocument web.xml add the following to the uncommented section:

```
<filter-mapping>
  <filter-name>authFilter</filter-name>
  <url-pattern>/opendoc/logonTrustedAuth.do</url-
pattern>
</filter-mapping>
```


8. Find the following parameters and make the appropriate changes:

<param-name>	Original <param-value>	New <param-value>
idm.realm	YOUR_REALM	Default realm for AD. This should be the same value you set when you configured the default_realm in your <code>krb5.ini</code> file. The value must be in upper case.
idm.princ	YOUR_PRINCIPAL	The SPN you created in To create an SPN for your web application server . It must follow the format: <code>HTTP/url</code> where <code>url</code> is the URL your users will use to access InfoView.
idm.allowNTLM	false	false
idm.allowUnsecured	true	true, unless you plan to use SSL

9. Add the `idm.keytab` parameter. In the Vintela section of the `web.xml` file add the following lines.

Note:

- Place it after the `idm.princ` parameter and values.

```
<init-param>
<param-name>idm.keytab</param-name>
<param-value>PATH_TO_YOUR_KEYTAB_FILE</param-value>
</init-param>
```

Where `Path_To_Your_Keytab_File` is the directory path to the location of your keytab file. For example, `C:\WINNT\host.keytab`

- Only add the above parameter if you have chosen to use a keytab file. If you have chosen to use a password do not add this parameter.

10. Save and close the file, then restart your web application server.

Note:

If you are using WebLogic, go to [To modify the web.xml in the war package](#).

Special considerations for WebLogic

If you are using WebLogic as your application server, you may not find the commented section in the Vintela xml properties that is mentioned in [To enable Vintela single sign-on for Java in the web.xml file](#). This is because WebLogic Builder, which is used in preparing the war files for deployment, removes the commented portions of the web.xml file.

Therefore, you must add the following xml to the web.xml file before proceeding with Step 5.

```
<filter>
  <filter-name>authFilter</filter-name>
  <filter-class>com.businessobjects.sdk.credential.Wrappe
dResponse
  AuthFilter</filter-class>
  <init-param>
    <param-name>idm.realm</param-name>
    <param-value>YOUR_REALM</param-value>
  </init-param>
  <init-param>
    <param-name>idm.princ</param-name>
    <param-value>YOUR_PRINCIPAL</param-value>
  </init-param>
  <init-param>
    <param-name>idm.allowUnsecured</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>idm.allowNTLM</param-name>
    <param-value>false</param-value>
  </init-param>
  <init-param>
    <param-name>idm.logger.name</param-name>
    <param-value>simple</param-value>
    <description>The unique name for this logger.</de
scription>
  </init-param>
  <init-param>
    <param-name>idm.logger.props</param-name>
```

```

    <param-value>error-log.properties</param-value>
    <description>Configures logging from the
        specified file.</description>
</init-param>

```

For InfoView include the following:

```

<init-param>
  <param-name>error.page</param-name>
  <param-value>/InfoView/logon/vintelaError.jsp
  </param-value>
  <description>The URL of the page to show if an error
      occurs during authentication.</description>
</init-param>
</filter>
<filter-mapping>
  <filter-name>authFilter</filter-name>
  <url-pattern>/InfoView/logon/logon.do</url-pattern>
</filter-mapping>

```

For OpenDocument include the following:

```

<init-param>
  <param-name>error.page</param-name>
  <param-value>/opendoc/vintelaError.jsp
  </param-value>
  <description>The URL of the page to show if an error
      occurs during authentication.</description>
</init-param>
</filter>
<filter-mapping>
  <filter-name>authFilter</filter-name>
  <url-pattern>/opendoc/logonVintela.do</url-pattern>
</filter-mapping>
<filter-mapping>
  <filter-name>authFilter</filter-name>
  <url-pattern>/opendoc/logonTrustedAuth.do</url-pattern>
</filter-mapping>

```

Return to [To enable Vintela single sign-on for Java in the web.xml file](#) and complete the steps there.

To modify the web.xml in the war package

Note:

Whenever you restart WebLogic, the `web.xml` will be overwritten and you will lose the above section. To avoid this issue, you can modify the `web.xml` in the actual war package for InfoView or OpenDocument. The `InfoViewApp` war file is used as an example in the following steps.

1. Locate the `InfoViewApp.war` file.

On Windows, the file is located at `<INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\java\applications`. If you did not modify the default installation location, replace `<INSTALLDIR>` with `C:\Program Files\`.

2. Create a folder called `WEB-INF` and place the modified `web.xml` file in this folder.

Note:

You must configure the `web.xml` file with the steps described in [To enable Vintela single sign-on for Java in the web.xml file](#) first.

3. Open a command window.
4. Change directories to the folder containing the `InfoViewApp.war`.
5. Execute the following command:

```
<INSTALLDIR>\javasdk\bin\ -uf InfoViewApp.war  
WEB-INF/web.xml
```

If you did not modify the default installation location, replace `<INSTALLDIR>` with `C:\Program Files\Business Objects`.

6. Return to [To enable Vintela single sign-on for Java in the web.xml file](#) and complete the tasks outlined there.

Setting up multiple SPNs

This step is optional. If you want to use single sign-on to InfoView with various URLs, you need to complete this step. For example, you need to perform these steps if you want your users to access an application server from a load-balanced URL, but you want administrators to access the application server directly.

Note:

This section assumes you have already completed steps 2 and 3. For a complete list of steps, see [Workflow for configuring Kerberos single sign-on to Java InfoView](#).

For each additional URL that you want to enable single sign-on to InfoView for, you need to add additional SPN mappings to the service account you created in step 1. Run the following command:

```
setspn -A HTTP/<myurl>@<REALM> -mapuser <user>
```

where

- **<myurl>** is the URL that your users will access InfoView with. For example, if the URL is `http://examplemachine.exampledomain.com:8080/InfoViewApp/` then **myurl** must be: `examplemachine.exampledomain.com`.
- **<REALM>** is the Active Directory realm in which the server is located. (For example, `EXAMPLE.COM`).
- **<user>** is the logon name of the user account you created in Step 1.

To increase the header size limit of your Java application server

Active Directory creates a Kerberos token which is used in the authentication process. This token is stored in the HTTP header. Your Java application server will have a default HTTP header size. To avoid failures, ensure that it has a minimum default size of 16384 bytes. (Some deployments may require a larger size. For more information, see Microsoft's sizing guidelines on their support site (<http://support.microsoft.com/kb/327825>).)

1. On the server with Tomcat installed, open the `server.xml` file.

On Windows, this file is located at `<TomcatINSTALLDIR>/conf`

- If you are using the version of Tomcat installed with BusinessObjects Enterprise on Windows, and you did not modify the default installation location, replace `<TomcatINSTALLDIR>` with `C:\ProgramFiles\Business Objects\Tomcat\`
- If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path.

2. Find the corresponding `<Connector ...>` tag for the port number you have configured.

If you are using the default port of 8080, find the `<Connector ...>` tag with `port="8080"` in it.

For example:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. Add the following value within the `<Connector ...>` tag:

```
maxHttpHeaderSize="16384"
```

For example:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25"
port="8080" redirectPort="8443" />
```

4. Save and close the `server.xml` file.
5. Restart Tomcat.

Note:

For other Java application servers, consult your Java application server's documentation.

Controlling logging with Vintela single sign-on for Java

Vintela single sign-on for Java uses Apache log4j logging. The name of the log file and the level of logging recorded are controlled by these:

- The settings related to Vintela logging in the `web.xml` for InfoView.
- The setting in the log4j properties file.

For more efficient problem determination, you may want to use the log files that are used to capture error or warning messages.

The table which follows summarizes what you can control about error logging with Vintela in the `web.xml` file for InfoView:

<param-name>	Use of parameter
idm.logger.name	The name of the log file is specified in the <param-value> for this parameter. This must be a unique name not in used by any other implementation of log4j logging on your web application.
idm.logger.props	<p>The <param-value> for this parameter can be set to three things: "" (blank), "BASIC" or "AnythingElse".</p> <ul style="list-style-type: none">• If the <param-value> for <code>idm.logger.props</code> is set to "" (blank), no logging will be performed.• If the <param-value> for <code>idm.logger.props</code> is set to "BASIC", basic errors will be logged and errors will be sent to the standard output.• If the <param-value> for <code>idm.logger.props</code> is set to anything other than "" or "BASIC", Vintela will look for a properties file that matches the value you set. Vintela will look for this properties file in the WEB-INF directory for InfoView. For example, if you specify BOE for your <param-value>, Vintela will look in the WEBINF directory for Infoview for the <code>BOE.properties</code> file.

What to specify in your log4j properties file

If you specify that you want to use a properties file in the <param-value> for `idm.logger.props` in the `web.xml` file for InfoView, you must also

create the properties file you specified in the WEB-INF directory for InfoView. These are the basic requirements:

- Defining which logger to use.
- Defining what level of logging to perform in this properties file.

For details on the syntax to use in the file and details on the of valid options of an Apache log4j properties file, see the following URL:

<http://logging.apache.org/log4j/1.2/apidocs/index.html>

To change the level of logging provided with Vintela single sign-on for Java

1. Open the web.xml file for InfoView from its deployed location on your web application server.

This is where the InfoView web.xml file is on Windows:

```
<INSTALLDIR>\businessobjects\enterprise120\desktop  
launch\WEB-INF
```

- If you are using the version of Tomcat installed with BusinessObjects Enterprise on Windows, and you did not modify the default installation location, replace `<INSTALLDIR>` with `C:\Program Files\Business Objects\Tomcat\webapps`
 - If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path.
2. If you want to have the output from error logging written to a file, find this string:

```
<param-name>idm.logger.name</param-name>
```

3. In the `<param-value>` for `idm.logger.name`, enter the name for your log file.
4. If you want to use a properties file to define the logger used and level of logging recorded, find this string:

```
<param-name>idm.logger.props</param-name>
```


5. In the `<param-value>` for `idm.logger.props`, enter the name for your properties file.

Note:

If you set this value to anything other than `<blank>` or “BASIC”, you must also define the logger used and define level of logging in the properties file you specify. For details, on the logging parameters available, see the table in the section [Controlling logging with Vintela single sign-on for Java](#).

6. Save and close your file.

Alternate URL to access InfoView

A second URL is available to access InfoView. This URL is provided for the administrator or a user to access InfoView, without single sign-on, after single sign-on has been enabled.

- This is the default URL used to access InfoView:

```
http://hostname:8080/InfoViewApp/logon.jsp
```

- This is the URL you should use if you want to access InfoView without single sign-on, after single sign-on has been enabled:

```
http://hostname:8080/InfoViewApp/logonNoSso.jsp
```

Modifying the Vintela logon error page

When authentication using Vintela single-sign-on for Java fails, Internet Explorer will attempt NTLM authentication. This will happen each time another logon attempt is made until the browser session ends, even if the underlying cause of failure has been resolved. To reduce the number of support calls received by an administrator, an error page will be displayed for the user.

This error page informs users of this behavior and instructs them to close their browser so that the next attempt can be successful, provided the underlying cause of the problem has been resolved.

To customize the text displayed on the Vintela error page

1. Open the file `vintelaError.jsp` file found in this location:

```
<INSTALLDIR>\businessobjects\enterprise120\desktop\plaunch\InfoView\logon\
```

If you installed Tomcat with your installation, and did not modify the default location, you can replace `INSTALLDIR` with this:

```
C:\Program Files\Business Objects\Tomcat\webapps
```

If you modified the default location for Tomcat, or used another supported Java application server, substitute the path applicable for deployment.

2. Change the text of the message as required.
3. Save and close the file.
4. Restart your web application server.

A second URL is available to access InfoView. This URL is provided for the administrator or a user to access InfoView, without single sign-on, after single sign-on has been enabled.

- This is the default URL used to access InfoView:

```
http://HostName:portnumber/businessobjects/enterprise120/desktoplaunch/InfoView/logon/logon.do
```

- This is the URL you should use if you want to access InfoView without single sign-on, after single sign-on has been enabled:

```
http://HostName:portnumber/businessobjects/enterprise120/desktoplaunch/InfoView/logon/logonForm.do
```

Configuring Internet browsers

To support Kerberos single sign-on, you must configure BusinessObjects Enterprise clients. This involves configuring the Internet Explorer (IE) browser on the client machines.

Note:

You can automate this through a registry key or use the following steps.

To configure Internet Explorer on the client machines

1. On the client machine open and IE browser window.
2. Enable integrated Windows authentication.
 - a. On the **Tools** menu click **Internet Options**.
 - b. Click the **Advanced** tab.

- c. Scroll to **Security**, select **Enable Integrated Windows Authentication**, and then click **Apply**.
3. Add the Java Application machine or the URL to the trusted sites. You can enter the full domain name of the site.
 - a. On the **Tools** menu click **Internet Options**.
 - b. Click the **Security** tab.
 - c. Click **Sites** and then click **Advanced**.
 - d. Type the web site for IIS and click **Add**.
 - e. Click **OK** until the Internet Options dialog box closes.
4. Close and reopen the Internet Explorer browser window for these changes to take effect.
5. Repeat all of these steps on each BusinessObjects Enterprise client machine.

To configure Firefox on the client machines

1. **Modify network.negotiate-auth.delegation-uris**
 - a. On the client machine open a Firefox browser window.
 - b. Type about:config in the URL address field. A list of configurable properties appears.
 - c. Double-click **network.negotiate-auth.delegation-uris** to edit the property.
 - d. Enter the URL that you will use to access InfoView. For example if your InfoView URL is `http://machine.domain.com:8080/InfoViewApp`, then you will need to enter `http://machine.domain.com`

Note:

To add more than one URL, separate them with a comma. For example: `http://machine.domain.com,machine2.domain.com`.

- e. Click **OK**.
2. **Modify network.negotiate-auth.trusted-uris**
 - a. On the client machine open a Firefox browser window.
 - b. Type about:config in the URL address field. A list of configurable properties appears.
 - c. Double-click **network.negotiate-auth.trusted-uris** to edit the property.
 - d. Enter the URL that you will use to access InfoView. For example if your InfoView URL is `http://machine.domain.com:8080/InfoViewApp`, then you will need to enter `http://machine.domain.com`

Note:

To add more than one URL, separate them with a comma. For example: `http://machine.domain.com,machine2.domain.com`.

- e. Click **OK**.
3. Close and reopen the Firefox browser window for these changes to take effect.
4. Repeat all of these steps on each BusinessObjects Enterprise client machine.

Modifying the web.config file for InfoView AD single sign-on

If you want to have AD single sign-on for InfoView, you must modify the web.config file for the following reasons:

- To change the authentication mode used.
- To allow impersonation.
- To enable single sign-on.
- To specify the authentication default.

These changes are in addition to changing how IIS is configured.

Note:

The values in web.config file are case-sensitive.

To modify web.config for AD single sign-on

1. Open the `web.config` file from this location:

```
C:\Program Files\Business Objects\BusinessObjects  
Enterprise 12.0\Web Content\ InfoViewApp\InfoViewApp\
```

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Find the following line in the `<system.web>` block:

```
<Authentication mode="None" />
```

3. Replace `"None"` with `"Windows"`.

```
<authentication mode="Windows" />
```

4. Add the following line:

```
<identity impersonate="true" />
```

5. Find the following string:

```
<add key="cmsDefault" value="" />
```

6. Enter the CMS machine in the `cmsDefault` `value` field.

7. Find the following string:

```
<add key=" ssoEnabled" value="false" />
```

8. Change the `ssoEnabled` value from `false` to `true`.

9. Find the following string:

```
<add key="authenticationDefault" value="secWinAD" />
```

10. Ensure the value for `authenticationDefault` is set to `secWinAD`.

11. Save and close the file.

12. Restart IIS.

Note:

For AD single sign-on to function correctly, make sure you complete all tasks listed in [Configuring Kerberos and single sign-on for .NET InfoView](#).

Modifying the web.config file for impersonation and Windows authentication

If you want to use AD authentication, you must modify the `web.config` file to change the authentication mode used and allow impersonation. This is in addition to changing how IIS is configured.

Modify either of the following `web.config` files based on what application you want to configure.

- To configure both the CMC and InfoView, configure the `web.config` file in the Web Content directory.

To configure only InfoView, configure the `web.config` file in the InfoView directory.

Note:

The values in `web.config` file are case-sensitive.

To modify web.config for basic AD authentication

1. Open the appropriate `Web.config` file from either of the following locations:
 - `C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Web Content\`
 - `C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp`

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Find the following line in the `<system.web>` block:

```
<authentication mode="None" />
```

3. Replace "None" with "Windows".

```
<authentication mode="Windows" />
```

4. Add the following line:

```
<identity impersonate="true" />
```

5. Save and close the file.
6. Restart IIS.

Configuring Kerberos and single sign-on to the database for Java application servers

Single sign-on to the database is supported for deployments that meet all these requirements:

- The deployment of BusinessObjects Enterprise is on a Java web application server.
- The Java web application server has been configured with AD with Kerberos.
- The database to which single sign-on is required is a supported version of SQL Server or Oracle.
- The groups or users that need access to the database must have been granted permissions within SQL Server or Oracle.

- The Cache Security context check box (which is required for single sign-on to the database) in the AD Authentication page of the CMC is checked.

The final step is to modify the `krb5.ini` file to support single sign-on to the database for Java.

Note:

These instructions explain how to configure single sign-on to the database for Java application servers. If you want to configure end-to-end single sign-on to the database for Java application servers, you must also perform the configuration steps required for Vintela single sign-on for Java. For details, see [Configuring Kerberos and single sign-on for Java InfoView](#).

Note:

If you want to configure single sign-on to a database, ensure that you have set the cache security context. For detailed instructions, go to [Enabling Kerberos authentication in the Windows AD plug-in](#).

To enable single sign-on to the database for Java application servers

1. Open the `krb5.ini` file that is being used for your deployment of BusinessObjects Enterprise.

The default location for this file is the WINNT directory on your web application server.

Note:

If you cannot find the file in the WINNT directory, check this Java argument for the location of the file:

```
-Djava.security.auth.login.config
```

This variable is specified when AD with Kerberos is configured on your Java web application server.

2. Go to the `[libdefaults]` section of the file.
3. Enter this string prior to the start of the `[realms]` section of the file:

```
forwardable = true
```

4. Save and close the file.
5. Restart your web application server.

Configuring Kerberos and single sign-on for .NET InfoView

This section described the steps required to configure single sign-on and AD authentication using Kerberos for BusinessObjects Enterprise .NET InfoView.

Before implementing these steps, make sure the manual authentication to .NET InfoView with Kerberos is working correctly. AD users must be able to provide their AD username and password to logon to .NET InfoView, and Kerberos has been enabled in the CMC.

Related Topics

- [Enabling Kerberos authentication in the Windows AD plug-in](#)
- [Configuring Kerberos for .NET InfoView and IIS](#)

To enable single sign-on in the CMC

1. Go to the "Authentication" management area of the CMC.
2. Double-click **Windows AD**.
3. Select **Enable Single Sign On for selected authentication mode** in the "Authentication Options" area.
4. Click **Update**.

Modifying web.config for impersonation and Windows authentication

To enable impersonal and Windows authentication, you need to modify the `Web.config` files for the two applications listed in the table below.

Application	Default location
InfoViewApp	<INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp
PlatformServices	<INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\PlatformServices

To modify web.config for impersonation and Windows authentication

1. Open the `Web.config` file for InfoView.

2. Locate the following line under `<system.web>`:

```
<Authentication mode="None" />
```

3. Modify the line as shown below:

```
<authentication mode="Windows" />
```

4. Locate the following line under `<system.web>`:

```
<identity impersonate="true" />
```

5. Edit the strings as indicated in the table below:

String	What to edit
<code><add key="cmsDefault" value="" /></code>	Enter the CMS machine name in the <code>cmsDefault</code> value field.
<code><add key=" ssoEnabled" value="false" /></code>	Change "false" to "true"
<code><add key="authenticationDefault" value="secWinAD" /></code>	Ensure value is set to "secWinAD"

6. Save and close the `Web.config` file.
7. Open the `Web.config` file for PlatformServices.
8. Edit the lines under `<system.web>` as indicated in the table below:

Line	What to edit
<code><Authentication mode="None" /></code>	Change "None" to "Windows"
<code><identity impersonate="true" /></code>	Ensure this line is set to "true"

9. Save and close the `Web.config` file.
10. Restart IIS.

Tip:

You can also restart IIS after you finish configuring IIS to use Integrated Windows Authentication.

To configure clients on IIS for Integrated Windows Authentication

To support single sign-on you need to configure the BusinessObjects Clients on IIS to use Integrated Windows Authentication. Implement the steps below to configure the clients for Windows authentication.

1. In the "Internet Information Services" window for IIS, expand the tree on the left and to `InfoViewApp` under **Default Web Site**.
2. Right-click **InfoViewApp** and select **Properties**.
3. Click **Edit** in the "Directory Security" tab.
4. Unselect **Anonymous Access** if it is selected
5. Select **Integrated Windows Authentication** and click **OK**.
6. Click **OK** to finish.
7. Repeat steps 1-6 for `PlatformServices`.
8. Restart IIS.

To configure the IIS host to be trusted for delegation

You must ensure that either the machine hosting IIS must be trusted for delegation, or the account IIS is running under must be trusted for delegation. Implement the steps below to configure the machine hosting IIS for delegation. For instructions on how to set the account IIS is running under please refer to your Windows AD documentation.

1. Open the "Active Directory Users and Computers" snap in.
2. Expand the tree to the domain of the machine hosting IIS.
3. Double click **Computers**.
4. Right-click the machine hosting IIS and select **Properties**
5. Select the "Delegation" tab.
6. Select **Trust this computer for delegation to any service (Kerberos only)** and click **OK**.

To configure the Internet Explorer browser

You need to configure the Internet Explorer browser on a BusinessObjects Enterprise client machine to support end-to-end single sign-on. This implementation includes the following tasks:

- Configuring client machines for integrated Windows authentication
- Adding IIS to the local intranet sites

Tip:

You can automate the following steps through a registry key. For more details, refer to your Windows documentation.

1. On the client machine, open an Internet Explorer browser.
2. Enable integrated windows authentication.
 - a. Go to **Tools > Internet Options**.
 - b. Select the "Advanced" tab.
 - c. Navigate to the "Security" settings.
 - d. Select **Enable integrated windows authentication** and click **Apply**.
3. Add IIS to the list of local intranet sites.
 - a. Go to **Tools > Internet Options**.
 - b. Go to **Security > Local intranet > Sites > Advanced**. "Security" tab.
 - c. Type in the web site for IIS, and click **Add**.
For example: `http://iismachine.domain.com`
 - d. Click **OK** twice to close the Internet Options dialog box.
4. Close the Internet Explorer browser, and then open it again for the changes to take effect.
5. Repeat steps 1-4 for every client machine.

Configuring Kerberos and single sign-on to the database for IIS

The setup single sign-on to the database, you need to configure IIS and BusinessObjects Enterprise to allow a users credentials to be propagated to the database. By implementing the steps in this section, users can have their AD account credentials authenticated against the underlying database. Before implementing end-to-end single sign-on, you must first complete the steps to set up single sign-on to .NET InfoView using Kerberos authentication. In addition, the following actions must be performed to setup single sign-on to the database:

1. The BusinessObjects Enterprise service account must be trusted for delegation.
2. Reporting Services must be running under the BusinessObjects Enterprise service account. The machines hosting the Reporting Services must have the BusinessObjects Enterprise service account as part of the local

Administrators group. The local security policy for the account must be set to “Act as part of the OS”.

3. **Cache security context** must be enabled. See [To configure the Windows AD security plug-in for Kerberos](#) for more details.
4. Configure IIS for access to the AD Domain Controller in order to perform queries.

Related Topics

- [Configuring Kerberos and single sign-on for .NET InfoView](#)
- [Setting up a service account](#)
- [Configuring the servers](#)

Configuring IIS for AD domain access

To support database single sign-on, you will have to set the `Aspnet_wp.exe` worker process to run as an account that has privileges connect to the Domain Controller. You can use any of the following choices:

- Run IIS worker process under a machine domain account. This way the password will automatically be generated and will not be subject to expiry restrictions. The password will not be exposed or subject to modification.
- Run IIS worker process under Network Service account or under as user domain account. By using a user domain account, you can control the rights of the account, however, the password can be exposed and modified. The password may also expire, and therefore cause errors.

The approach you use depends your system security management requirements. For complete information about security risks associated with system or user domain accounts, refer to your Microsoft documentation.

To configure IIS 5 for AD domain access

If IIS 5 is already running under a Domain account, System account or Network Service account, you can skip these steps.

1. Open the `machine.config` file.

This file can be found at the following location: `C:\Winnt\Microsoft.NET\Framework\version\CONFIG\`, where *version* represents the software version number.

2. Locate the `processModel Attributes` section in the file.
3. Set the parameter values indicated in the following table: .

Parameter	Value to set
userName	"Password"
Password	"AutoGenerate"

4. Save and close the file.

Configuring the `Aspnet_wp.exe` account to run as a machine domain account will cause all ASP.NET web applications on the web server to run as privileged system accounts. For security reasons, make sure that the account which IIS runs under does not belong to a mapped group.

If the machine name for the web server is different from the name that is used to access it, add an SPN for HTTP access on the web server machine:

```
setspn -A HTTP/serverhost.domainname.com serverhost
```

For example, if you access the machine via `www.domainname.com` but the machine name is `web.domainname.com`, you will have to add an a SPN for HTTP access on the web server machine.

To configure IIS 6 for AD domain access

IIS 6 should be running by default under the **Network Service** account which has sufficient rights for AD domain access..

1. To open the Internet Information Services (IIS) Manager go to: **Start > Settings > Control Panel > Administrative Tools**.
2. Go to **local computer > Application Pools**
3. Right-click **DefaultAppPool** and select **Properties**.

If BusinessObjects Enterprise is not installed in the default Application Pool, you should use the pool in which it is installed.

4. Select the "Identity" tab. Ensure that Network Services is selected and not any of the Local accounts.

Note:

You can alternatively use "Configurable" and run the Application Pool under a domain account.

5. Click **OK**.
6. Restart IIS if you modified any of the Application Pool settings.

Configuring NTLM and single sign-on for .NET InfoView

This section described the steps required to configure single sign-on and AD authentication using NTLM for BusinessObjects Enterprise .NET InfoView.

Before implementing these steps, make sure the manual authentication to .NET InfoView with NTLM is working correctly. AD users must be able to provide their AD username and password to logon to .NET InfoView, and Kerberos has been enabled in the CMC.

Related Topics

- [Using AD authentication with NTLM](#)

To enable single sign-on in the CMC

1. Go to the "Authentication" management area of the CMC.
2. Double-click **Windows AD**.
3. Select **Enable Single Sign On for selected authentication mode** in the "Authentication Options" area.
4. Click **Update**..

Modifying web.config for impersonation and Windows authentication

To enable impersonal and Windows authentication, you need to modify the `Web.config` files for the two applications listed in the table below.

Application	Default location
InfoViewApp	<INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp
PlatformServices	<INSTALLDIR>\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\PlatformServices\

To modify web.config for impersonation and Windows authentication

1. Open the `Web.config` file for InfoView.
2. Locate the following line under `<system.web>`:

```
<Authentication mode="None" />
```

3. Modify the line as shown below:

```
<authentication mode="Windows" />
```

4. Locate the following line under `<system.web>`:

```
<identity impersonate="true" />
```

5. Edit the strings as indicated in the table below:

String	What to edit
<code><add key="cmsDefault" value="" /></code>	Enter the CMS machine name in the <code>cmsDefault</code> value field.
<code><add key=" ssoEnabled" value="false" /></code>	Change "false" to "true"
<code><add key="authenticationDefault" value="secWinAD" /></code>	Ensure value is set to "secWinAD"

6. Save and close the `Web.config` file.
7. Open the `Web.config` file for PlatformServices.
8. Edit the lines under `<system.web>` as indicated in the table below:

Line	What to edit
<code><Authentication mode="None" /></code>	Change "None" to "Windows"
<code><identity impersonate="true" /></code>	Ensure this line is set to "true"

9. Save and close the `Web.config` file.
10. Restart IIS.

Tip:

You can also restart IIS after you finish configuring IIS to use Integrated Windows Authentication.

To configure clients on IIS for Integrated Windows Authentication

To support single sign-on you need to configure the BusinessObjects Clients on IIS to use Integrated Windows Authentication. Implement the steps below to configure the clients for Windows authentication.

1. In the "Internet Information Services" window for IIS, expand the tree on the left and to `InfoViewApp` under **Default Web Site**.
2. Right-click **InfoViewApp** and select **Properties**.
3. Click **Edit** in the "Directory Security" tab.
4. Unselect **Anonymous Access** if it is selected.
5. Select **Integrated Windows Authentication** and click **OK**.
6. Click **OK** to finish.
7. Repeat steps 1-6 for `PlatformServices`.
8. Restart IIS.

To configure the Internet Explorer browser

You need to configure the Internet Explorer browser on a BusinessObjects Enterprise client machine to support end-to-end single sign-on. This implementation includes the following tasks:

- Configuring client machines for integrated Windows authentication
- Adding IIS to the local intranet sites

Tip:

You can automate the following steps through a registry key. For more details, refer to your Windows documentation.

1. On the client machine, open an Internet Explorer browser.
2. Enable integrated windows authentication.
 - a. Go to **Tools > Internet Options**.
 - b. Select the "Advanced" tab.
 - c. Navigate to the "Security" settings.
 - d. Select **Enable integrated windows authentication** and click **Apply**.
3. Add IIS to the list of local intranet sites.
 - a. Go to **Tools > Internet Options**.
 - b. Go to **Security > Local intranet > Sites > Advanced**.
 - c. Type in the web site for IIS, and click **Add**.

For example: `http://iismachine.domain.com`

- d. Click **OK** twice to close the Internet Options dialog box.
4. Close the Internet Explorer browser, and then open it again for the changes to take effect.
5. Repeat steps 1-4 for every client machine.

Using AD with SiteMinder

This section provides information on different methods offered by BusinessObjects Enterprise that can be used for authentication with Windows Active Directory (AD) and SiteMinder for IIS and Java. Information on administering and configuring AD accounts is also included.

You can use SiteMinder with NTLM or Kerberos. For more information about NTLM, see [Using AD authentication with NTLM](#). For more information about Kerberos, see [Using AD authentication with Kerberos](#).

AD and SiteMinder workflow

The workflow for configuring BusinessObjects Enterprise to use IIS with AD and SiteMinder, involves these steps:

- [Mapping AD accounts](#)
- [Configuring the Windows AD plug-in for SiteMinder](#)
- [Modifying the web.xml for Java AD and SiteMinder](#)

Configuring AD and SiteMinder workflow

This section explains how to use AD and SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the AD security plug-in to create single sign-on to BusinessObjects Enterprise. This section assumes that you have completed [Mapping AD accounts](#).

There are two things you must do to enable AD single sign-on with SiteMinder:

- Configure the AD plug-in for single sign-on with SiteMinder
- Modify either the Web.xml file to use Java and SiteMinder or the Web.config file to use .NET and SiteMinder

Note:

Please ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done regardless of which supported version of

SiteMinder you are using. For more information about SiteMinder and how to install it, refer to the SiteMinder documentation.

Configuring the Windows AD plug-in for SiteMinder

To configure the AD plug-in for single sign-on with SiteMinder

1. From the CMC, click **Authentication**.
2. Double-click **Windows AD**.
3. Scroll down to the **SiteMinder options** area of the page.
4. Click **Disabled**.

The Windows AD SiteMinder configuration page will appear.

5. If you have not configured the Windows AD plug-in, you will receive a warning and will be asked if you wish to continue. Click **OK**.

The AD SiteMinder configuration page appears.

6. Click **Use SiteMinder Single Sign On**.
7. In the Policy Server Host box, type the name of each policy server, and click **Add**.
8. For each Policy Server Host, specify the **Accounting**, **Authentication** and **Authorization** port numbers.
9. Enter the name of the **Agent Name** and the **Shared Secret**. Enter the **Shared Secret** again.

Note:

Please ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done regardless of which supported version of SiteMinder you are using. For more information about SiteMinder and how to install it, refer to the SiteMinder documentation.

10. Click **Update**.

Modifying the web.xml for Java AD and SiteMinder

To enable Java AD SiteMinder

1. Open the web.xml file for InfoView, from its deployed location on your web application server.

```
<DeployedLocation>\Business Objects\BusinessObjects  
Enterprise 12.0\warfiles\  
warfiles\WebApss\InfoViewApp\WEB-INF
```

Note:

If you are using the version of Tomcat installed with BusinessObjects Enterprise, replace `<DeployedLocation>` with `C:\Program Files\Business Objects\tomcat55\webapps`. If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path to substitute.

2. Find the following string in the file:

```
<param-name>cms.default</param-name>
```

3. Enter the CMS name and port number in the `cms.default` `<param-value>` field.

Use the format `servername:portnumber`.

4. Find the following string in the file:

```
<param-name>authentication.default</param-name>
```

5. Set the `<param-value>` for the `authentication.default` to `secWinAD`.

```
<param-value>secWinAD</param-value>
```

6. Find the following string in the file:

```
<param-name>sso.enabled</param-name>
```

7. Change the `<param-value>` for `sso.enabled` from `false` to `true`.

```
<param-value>true</param-value>
```

8. Find the following string in the file:

```
<param-name>siteminder.enabled</param-name>
```

9. Change the `<param-value>` for `siteminder.enabled` from `false` to `true`.

```
<param-value>true</param-value>
```

10. Find the following string in the file:

```
<param-name>siteminder.authentication</param-name>
```

11. Set the `<param-value>` for `siteminder.authentication` to `secWinAD`.

```
<param-value>secWinAD</param-value>
```

12. Save and close the file.
13. Restart your web application server.

Modifying the web.xml for Java AD Single sign-on to InfoView

To enable Java AD single sign-on

1. Open the web.xml file for InfoView, from its deployed location on your web application server.

```
<DeployedLocation>\InfoViewApp\WEB-INF
```

Note:

If you are using the version of Tomcat installed with BusinessObjects Enterprise, replace `<DeployedLocation>` with `C:\Program Files\Business Objects\tomcat55\webapps`. If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path to substitute.

2. Find the following string in the file:

```
<param-name>cms.default</param-name>
```

3. Enter the CMS name and port number in the `cms.default` `<param-value>` field.

Use the format `servername:portnumber`.

4. Find the following string in the file:

```
<param-name>authentication.default</param-name>
```

5. Set the `<param-value>` for the `authentication.default` to `secWinAD`.

```
<param-value>secWinAD</param-value>
```

6. Find the following string in the file:

```
<param-name>sso.enabled</param-name>
```

7. Change the `<param-value>` for `sso.enabled` from `false` to `true`.

```
<param-value>true</param-value>
```

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

Modifying the web.xml file for Java AD and SiteMinder

To enable the Java AD client for SiteMinder

1. Open the `web.xml` file for InfoView, from its deployed location on your web application server.

```
<DeployedLocation>\InfoViewApp\WEB-INF
```

Note:

If you are using the version of Tomcat installed with BusinessObjects Enterprise, replace `<DeployedLocation>` with `C:\Program Files\Business Objects\tomcat55\webapps`. If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path to substitute.

2. Find the following string in the file:

```
<param-name>cms.default</param-name>
```

3. Enter the CMS name and port number in the `cms.default` `<param-value>` field.

Use the format `servername:portnumber`.

4. Find the following string in the file:

```
<param-name>authentication.default</param-name>
```

5. Set the `<param-value>` for the `authentication.default` to `secWinAD`.

```
<param-value>secWinAD</param-value>
```

6. Find the following string in the file:

```
<param-name>sso.enabled</param-name>
```

7. Change the <param-value> for sso.enabled from false to true.

```
<param-value>true</param-value>
```

8. Find the following string in the file:

```
<param-name>siteminder.enabled</param-name>
```

9. Change the <param-value> for siteminder.enabled from false to true.

```
<param-value>true</param-value>
```

10. Find the following string in the file:

```
<param-name>siteminder.authentication</param-name>
```

11. Set the <param-value> for siteminder.authentication to secWinAD.

```
<param-value>secWinAD</param-value>
```

12. Save and close the file.
13. Restart your web application server.

Modifying web.config for .NET InfoView and SiteMinder

To enable .NET InfoView client for SiteMinder

1. Open the web.config file for InfoView, from its deployed location for IIS.

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp
```

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Find the following string in the file:

```
<add key="cmsDefault" value="" />
```

3. Enter the CMS name in the `cmsDefault` value field.
4. Find the following string in the file:

```
<add key="authenticationDefault" value="secEnterprise" />
```

5. Set the value for the `authenticationDefault` to `secWinAD`.
6. Find the following string in the file:

```
<add key="ssoEnabled" value="false" />
```

7. Change the value for `ssoEnabled` from `false` to `true`.
8. Find the following string in the file:

```
<add key="siteminderEnabled" value="true" />
```

9. Ensure the value for `siteminderEnabled` is set to `true`.
10. Find the following string in the file:

```
<add key="siteminderAuthentication" value="secLDAP" />
```

11. Set the value for `siteminderAuthentication` to `secWinAD`.

```
<param-value>secWinAD</param-value>
```

12. Save and close the file.
13. Restart IIS.

Disabling SiteMinder for Java clients

If you want to prevent SiteMinder from being configured, or to disable it after it has been configured in the CMC, modify the `web.xml` file for InfoView.

To modify `web.xml` to disable SiteMinder

1. Open the `web.xml` file for InfoView on your web application server.

```
<DeployedLocation>\InfoViewApp\WEB-INF
```

Note:

If you are using the version of Tomcat installed with BusinessObjects Enterprise, replace `<DeployedLocation>` with `C:\Program Files\Business Objects\tomcat55\webapps`. If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path to substitute.

2. Find the following string in the file:

```
<param-name>siteminder.enabled</param-name>
```

3. Change the `<param-value>` from `true` to `false`.

```
<param-value>>false</param-value>
```

4. Save and close the file.
5. Restart your web application server.

Disabling SiteMinder for .NET clients

If you want to prevent SiteMinder from being configured, or to disable it after it has been configured in the CMC for .NET, modify the `web.config` file for InfoView.

To modify web.config to disable SiteMinder for .NET clients

1. Open the `web.config` file for InfoView on your web application server.

```
C:\Program Files\Business Objects\BusinessObjects  
Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp
```

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Find the following string in the file:

```
<add key="siteminderEnabled" value="true" />
```

3. Change the value from `true` to `false`.

```
<param-value>>false</param-value>
```

4. Repeat steps 1-3 for the `web.config` file for PlatformServices:


```
C:\Program Files\Business Objects\BusinessObjects  
Enterprise 12.0\Web  
Content\InfoViewApp\PlatformServices
```

5. Save and close the file.
6. Restart IIS.

Troubleshooting single sign-on

This section contains some of the common configuration errors which can single sign-on not to function properly.

- Disabled single sign-on
- Security context problem
- Duplicate ssoEnabled tags

Disabled single sign-on

Despite the fact that single sign-on has been configured in the web.config files, users receive the following error:

```
The administrator has disabled Single Sign-On logons for  
this authentication plugin. Please log on using your  
username and password.
```

This problem occurs when single sign-on configuration is missing from the CMC but present in all the other required locations.

To enable single sign-on in the CMC

1. Go to the **Authentication** area of the CMC.
2. Double-click **Windows AD**.
3. In the Authentication Options area of the page, select "**Enable Single Sign On for selected authentication mode.**"
4. Restart the IIS.

Security context issues

After single sign-on has been set up, when the users attempt to access InfoView, they receive the following error:

```
An error has occurred propagating the security context
between the security server and the client. Please con-
tact your system administrator.
```

This can be caused because the impersonation setting has been set incorrectly or the setting is missing from the web.config file.

To resolve security context issues

1. Open the web.config file at this location:

```
C:\Program Files\Business Objects\BusinessObjects En-
terprise 12.0\Web Content\InfoViewApp
```

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Make sure both of these lines exist in the file.

```
<authentication mode="Windows"/>
<identity impersonate="true" />
```

If either line is missing, add it. If either has a different setting, change it to match the required setting.

3. Save and close the file
4. Repeat steps 1-3 for the web.config file for PlatformServices:

```
C:\Program Files\Business Objects\BusinessObjects
Enterprise 12.0\Web
Content\InfoViewApp\PlatformServices
```

5. Restart IIS.

Duplicate ssoEnabled tags

Single sign-on has been configured in the web.config files, but the InfoView Log on screen appears with a blank user name and password, and with Windows AD authentication selected. After you click **Log on**, you are logged on successfully. No error message is displayed.

This can occur if you have multiple contradictory values set for the key `ssoEnabled` in the `web.config` file. Consider the following sample where the `ssoEnabled` is set twice: the first time it is set to `true`, the second time it is set to `false`.

```
<add key="cmsDefault" value="ABCADEI01" />
<add key="ssoEnabled" value="true" />
<add key="authenticationDefault" value="secWinAD" />
<add key="cmsVisible" value="true" />
.
<!-- Set to false to disable Siteminder sso -->
<add key="siteminderEnabled" value="true" />
<add key="siteminderAuthentication" value="secLDAP" />
<!-- Set to true to enable other Single Sign On -->
<add key="ssoEnabled" value="false" />
```

To remove the duplicate tag

1. Open the `web.config` file from the following location:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Web Content\InfoViewApp\InfoViewApp
```

Note:

The path mentioned is the default location. Modify your path accordingly if you changed the default location.

2. Search for the following throughout the file:

```
ssoEnabled
```

3. If you find multiple occurrences, ensure the first one has the setting you want, then delete the duplicate tags.
4. Save and close the file.
5. Restart IIS.

Enabling Trusted Authentication

Users prefer to log on to the system once, without needing to provide passwords several times during a session. Trusted Authentication provides a Java single sign-on solution for integrating your BusinessObjects Enterprise authentication solution with third-party authentication solutions. Applications that have established trust with the Central Management Server can use

Trusted Authentication to allow users to log on without providing their passwords. To enable Trusted Authentication, you must configure both the server, through the CMC, and the client, in the web.xml file.

If you are using Business Process BI Web Service, you also must configure the BusinessProcessBI.properties file. See for details.

Note:

- Before you are able to use Trusted Authentication, you must have either created Enterprise users, or mapped the third-party users that will need to sign on to BusinessObjects Enterprise.
- The SSO URL for Java InfoView is: `http://hostname:portnumber/InfoViewApp/logon/logon.do`
- The SSO URL for .NET InfoView is `http://hostname:portnumber/InfoViewApp/logon/logon.aspx`

Related Topics

- [Configuring the server for Trusted Authentication](#)
- [Configuring Trusted Authentication for the client](#)
- [Configuring Trusted Authentication for Business Process BI](#)

Configuring the server for Trusted Authentication

To configure the server to use Trusted Authentication

1. Log on to the Central Management Console with administrative rights.
2. Go to the **Authentication** management area of the CMC.
3. Click the **Enterprise** tab.
4. Scroll down until you see Trusted Authentication.
5. Click **Trusted Authentication is enabled**.
6. Enter a string in the **Shared Secret** field.

Note:

The shared secret is used by the client and the CMS to establish trust. You must also configure the client after you finish the Trusted Authentication configuration for the server. See [Configuring Trusted Authentication for the client](#) for details.

7. To specify the number of days that your shared secret will be valid, specify a value for the **Shared Secret Validity Period** field.
8. Specify a timeout value for your trusted authentication requests.

Note:

The timeout value is the maximum amount of time, in milliseconds, that the clock on the client and clock and the CMS can differ. If you enter 0, the amount of time the two clock times can differ is unlimited. It is not recommended you set this value to 0 as this may increase your vulnerability to replay attacks.

9. Click **Update**.

Configuring Trusted Authentication for the client

To configure Trusted Authentication for the client

The following procedure can be used for both the InfoView and OpenDocument web applications.

1. Open the `web.xml` file for InfoView or OpenDocument from the deployed location on your web application server.

The deployed location for InfoView on Windows is:

```
<DeployedLocation>\Business Objects\BusinessObjects  
Enterprise  
12.0\warfiles\WebApps\InfoViewApp\WEB-INF
```

The deployed location for OpenDocument is:

```
<DeployedLocation>\Business Objects\BusinessObjects  
Enterprise  
12.0\warfiles\WebApps\OpenDocument\WEB-INF
```

In Steps 2-14 InfoView will be the assumed web application.

Note:

If you have InfoView deployed in a .NET environment, the `web.config` is located in the following directory:

```
<DeployedLocation>\Business Objects\BusinessObjects  
Enterprise  
12.0\Web Content\InfoViewApp\InfoViewApp\
```

2. Find this string in the file:

```
<param-name>cms.default</param-name>
```

3. Enter the CMS name and port number in the `cms.default` `<param-value>` field.

Use the format `servername:portnumber`

4. Find this string in the file:

```
<param-name>sso.enabled</param-name>
```

5. Change the `<param-value>` for `sso.enabled` from `false` to `true`.

```
<param-value>true</param-value>
```

6. Find this string in the file:

```
<param-name>siteminder.enabled</param-name>
```

7. Change the `<param-value>` for `siteminder.enabled` from `true` to `false`.

```
<param-value>>false</param-value>
```

8. Find this string in the file:

```
<param-name>trusted.auth.user.retrieval</param-name>
```

9. Specify how you want to retrieve the user name.

Enter the `<param-value>` from the table that corresponds with the user retrieval method you want to use.

<param-value>	How the User name will be retrieved
REMOTE_USER	<p>The user name will be retrieved from a call to <code>getRemoteUser()</code> on the <code>HttpServletRequest</code> object for the current request in a servlet or JSP.</p> <p>Note: For .NET, ensure that the following properties have been set on your <code>InfoViewApp</code> directory:</p> <ul style="list-style-type: none"> • In IIS manager, disable the "anonymous access" check box. • In IIS manager, enable the "Windows Integrated Authentication" check box.
HTTP_HEADER	<p>The user name is retrieved from the contents of a specified HTTP header.</p> <p>Note: You must define which http header you want to use to retrieve the user name. You define the http header to use is defined in the <code>trusted.auth.user.param</code> in the <code>web.xml</code> file for InfoView.</p>

<param-value>	How the User name will be retrieved
QUERY_STRING	<p>The user name is retrieved from the contents of contents of a specified parameter of the request URL.</p> <p>Note: You must define which query string parameter you want to use to retrieve the user name. You define query string parameter to use in the <code>trusted.auth.user.param</code> in the <code>web.xml</code> file for InfoView.</p>
COOKIE	<p>The user name is retrieved from the contents of contents of a specified cookie.</p> <p>Note: You must define which cookie you want to use to retrieve the user name. You define the cookie to use in the <code>trusted.auth.user.param</code> in the <code>web.xml</code> file for InfoView.</p>
WEB_SESSION	<p>The user name is retrieved from the contents of a specified session variable.</p> <p>Note: You must define which web session variable want to use to retrieve the user name. You define the web session variable to use in the <code>trusted.auth.user.param</code> in the <code>web.xml</code> file for InfoView.</p>

<param-value>	How the User name will be retrieved
USER_PRINCIPAL	The user name is retrieved from a call to <code>getUserPrincipal().getName()</code> on the <code>HttpServletRequest</code> object for the current request in a servlet or JSP.

Note:

- There are various mechanisms that populate the user name. Configure or set up your web application server so that your user names are exposed before you use these user retrieval name methods. See <http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html> for further information.
- Some web application servers require that you have the environment variable `REMOTE_USER` set to true on your web application server. See the documentation specific to your web application server for details on whether this is required. If it is required, ensure the environment variable is set to true if you are using this method of user name retrieval.

10. If you selected HTTP header, URL query string, cookie or web session, find this string:

```
<param-name>trusted.auth.user.param</param-name>
```

Note:

This step is not required if your retrieval method is `USER_PRINCIPAL` or `REMOTE_USER`.

11. Enter the variable name to use to retrieve the user name in the <param-value> for `trusted.auth.user.param`
- If you are using the HTTP header as your method of retrieving the user name, enter the name for the HTTP header variable.
 - If you are using a URL query string parameter as your method of retrieving the user name, enter the name for the parameter.

- If you are using a cookie as your method of retrieving the user name, enter the name for the cookie.
- If you are using a web session variable as your method of retrieving the user name, enter the name for the web session variable.

Note:

This step is not required if your retrieval method is `USER_PRINCIPAL` or `REMOTE_USER`.

12. Decide how you want to retrieve the shared secret.

To retrieve the shared secret from a file:

- Create a file called `TrustedPrincipal.conf`.
- Store the file in the platform specific directory of Business Objects.

This table specifies the location where the `TrustedPrincipal.conf` file should be stored, based on your platform.

Platform	Location of TrustedPrincipal.conf
Windows, default installation	C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\
Windows, modified default install directory	<code><INSTALLDIR> \BusinessObjects Enterprise 12.0\win32_x86</code> Note: Replace <code>INSTALLDIR</code> with your installation directory.
AIX	<code><INSTALLDIR>/bobje/enterprise120/aix_rs6000/</code>

Platform	Location of TrustedPrincipal.conf
Solaris	<INSTALLDIR>/bobje/enterprise120/solaris_sparc/
HP_UX	<INSTALLDIR>/bobje/enterprise120/hpux_pa-risc
Linux	<INSTALLDIR>/bobje/enterprise120/linux_x86/

- c. Define the string you want to use for the shared secret.

Enter the following in the file, where String is the shared secret string you want to use.

```
SharedSecret=String
```

- d. Save and close this file.

To retrieve the shared secret from a session variable:

- a. Find this string in the web.xml file:

```
<param-name>trusted.auth.shared.secret</param-name>
```

- b. Enter the session variable name from which to retrieve the shared secret in the </param-value> for trusted.auth.shared.secret.

Note:

Business Process BI Web Services does not support retrieving the shared secret from a session variable.

13. Save and close the file.
14. Restart your web application server.

Configuring Trusted Authentication for Business Process BI

If you are using Business Process BI and you are using Trusted Authentication, you must configure the BusinessProcessBI.properties file in addition to configuring the CMC and the web.xml.

To configure Trusted Authentication for Business Process BI

1. Open the BusinessProcessBI.properties file from the following location on your web application server:

For Windows:

```
<DeployedLocation>\BusinessProcessBI\WEB-INF\classes
```

For Unix:

```
<DeployedLocation>/BusinessProcessBI/WEB-INF/classes/
```

Note:

If you are using the version of Tomcat installed with BusinessObjects Enterprise, replace `<DeployedLocation>` with `C:\Program Files\Business Objects\Tomcat55\webapps\` on Windows, or the Tomcat directory on Unix. If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path to substitute.

2. Find this line:

```
bisecurity.trustedAuthentication.enabled = false
```

3. Change the value `false` to `true`.
4. Save and close the file.
5. Restart your web application server.



Working with Federation



7

chapter



Federation

Federation is an important cross-site replication tool for working with multiple BusinessObjects Enterprise deployments in a global environment.

Content can be created and managed from one BusinessObjects Enterprise deployment and replicated to other BusinessObjects Enterprise 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 is a flexible feature that allows you to have separate security models, life cycles, 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, etc.	All objects are supported, although not at the individual level.
Reports	Crystal reports, Web Intelligence, Full Client and Xcelsius	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, Custom Roles, Hyperlinks, Shortcuts, Programs, Profiles, MyInfoView, Object Packages, Agnostic	
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, which 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 set the reports to run on the Origin site before the completed report is sent back to the Destination site.

Federation terms

Federation, a new feature in the BusinessObjects Enterprise, is an important cross-site replication tool for working with BusinessObjects Enterprise objects in a global environment. 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 BusinessObjects Enterprise deployment can host multiple BI applications, each of which can have a separate security model, life cycle, testing and deployment timeline, as well as separate business owners and administrators.

Destination site

A BusinessObjects Enterprise system that pulls replicated BusinessObjects Enterprise 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 only be one Origin site per replication.

One-way replication

Objects are only replicated 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise 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, as shown here:  If there is a conflict, objects will be flagged with a conflict icon, as shown here: 

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.

Managing Replication Lists

A Replication List refers to other content such as users, groups, reports, and so on in the BusinessObjects Enterprise deployment to be replicated together. Replication Lists can be accessed from the CMC.

Content that can be replicated are listed in the following table.

Category	Supported objects
Repository objects	Objects that include Business Views, DataConnection, LOVs, Data Foundation, and more. Note: All objects are supported, although not at the individual level.
Reports	Crystal Reports, Web Intelligence and Full Client, and Xcelsius. Note: Full Client Addin and Templates are supported.
Third-party objects	Excel, PDFs, Powerpoint, Flash, Word, text files, rich text files, Shockwave Flash files
Users	Users, groups, Inboxes, Favorites, personal Category
Business Intelligence Platform	Folders, events, categories, calendars, custom roles, hyperlinks, shortcuts, programs, profiles, MyInfoView, object packages, agnostic
Universes	Universes, connections, universe overload

Note:

To ensure changes are made on both sites to the following objects, create Business Views, Business Elements, Data Foundations, Data Connections, List of Values, and Universe Overloads on the Origin site and then replicate them to the Destination site. However, 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.

Creating Replication Lists

Replication Lists are located in a separate folder than Federation in the CMC. To organize a Replication List, you may create folders and subfolders within the Replication List folder.

To create a Replication List folder

1. Go to the **Replication Lists** area of the **CMC**.

2. Click **Replication Lists**.
3. Click **Manage**.
4. Click **New**, and then click **Folder**.
A **Create Folder** dialog box opens.
5. Enter a folder name and select **OK**.

You can now create a Replication Lists object by selecting the folder you want it listed in.

To create a Replication List

1. Go to the **Replication Lists** area of the **CMC**.
2. Click desired **Replication Lists** folder where you would like to save your new **Replication List**.
3. Click **Manage**.
4. Click **New**, and then click **Create New Replication List**.
The **New Replication List** dialog box opens.
5. Enter the **Title** and **Description** of the Replication List.
For advanced options, expand the **Replication List Properties** link.

Note:

This allows you to specify which dependencies to automatically bring over. The default is all. If you deselect these options, you must manually select an object's dependent objects so they will work correctly on the Destination site.

6. Select the desired options as described in the table.
 - **Replicate all object dependencies**

Note:

- This is the default option. Dependencies include the following objects and their related dependencies: relationships: DataConnection, Universe: Web Intelligence Universe, User Group: User, Universe: Universe, CustomRole: Object, Profile: Principal, and User: Favorites folder.
- This option only brings dependencies supported by Federation.
- Include personal folders for selected users
- Include personal categories for selected users

- Include universes for selected reports
- Include members of selected user groups
- Include universes required by selected universes
- Include inboxes for selected users
- Include user groups for selected universes
- Include access levels set on selected objects
- Include documents for selected categories
- Include supported dependencies for selected Flash objects
- Include profiles for selected users and user groups
- Include connections used by selected universes

Note:

Objects in BusinessObjects Enterprise may be dependent on other objects. For example: a Web Intelligence document is dependent on the underlying universe for its structure, content, and so on. These dependencies are replicated automatically when an object is replicated to another BusinessObjects Enterprise system.

7. Select Next.

A **New Replication List** dialog box opens.

- 8.** Select the desired objects to add to your Replication List, which must contain at least one object.
- Add or remove options using the arrow buttons
 - Or click **Replicate all:Repository Objects** to replicate all Business View, Business Elements, Data Foundation, Data Connection, List of Values, and repository objects, including report images and functions

Dependency object options	Definition
universe for selected reports	Replicates any universe that selected report objects depend on. Note: If you replicate a universe from the Origin site to the Destination site, it will not remove any relationships it sent to “Destination only reports”. Therefore, you may want to create “Destination only reports” from replicated universes.
user groups that contain selected users	Brings the user groups that selected users are members of. Note: If you replicate a user group from the Origin site to the Destination site, it will not remove its memberships to “Destination only users”. Therefore, you may want to add “Destination only users” to a replicated group.
universes required by selected universes	Replicates any universe that depend on other universes.
profiles for selected users and user groups	Replicates any profiles associated with selected users or groups.
access levels set on selected objects	Replicates any access levels used on any of the selected objects.
connections used by selected universes	Replicates any universe connection objects used by selected objects. Note: If you replicate a universe connection from the Origin site to the Destination site, it will not remove any relationships it replicated to “Destination only universes”. Therefore, you may want to create “Destination only universes” that use replicated universe connections.
supported dependencies for selected Flash objects	Replicates any Crystal reports, hyperlinks, Web Intelligence reports or universes that the Flash object depends on.

Dependency object options	Definition
documents for selected categories	Replicates any documents, including Word, Excel, PDF, and so on that are included in selected categories. Note: If you replicate a category from the Origin site to the Destination site, it will not remove any relationships it may have replicated to “Destination only documents”. Therefore, you may want to add “Destination only documents” to replicated categories.
inboxes for selected users	Replicates a selected user's Inbox and its content.
personal folders for selected users	Replicates a selected user's personal folders and their content.
members of selected user groups	Replicates users within a selected group.
personal categories for selected users	Replicates a selected user's personal categories.
user groups for selected universes	Replicates the user groups associated with a universe's overloads.

Note:

It is not possible to replicate top level folders, which are located under the “Available Objects” folder.

For example, if you replicate a Web Intelligence report but do not select the universe it uses, replication will not work on the Destination site unless the universe was already replicated there. However, enable “Include Universes” for selected reports, and Federation brings the universe(s) that the report depends on.

Note:

If you add a Web Intelligence report to the Replication List and enable the universe dependency and the universe connection dependency, both the universe and report rely on the universe connection and are brought over by Federation.

9. Click **Save & Close**.

Modifying Replication Lists

Once you create a Replication List, you can modify its properties or objects.

To modify properties in a Replication List

1. Go to the **Replication Lists** area of the **CMC**.
2. Select a **Replication List**.
3. On the **Manage** menu, click **Properties**.
The **Properties** dialog box opens.
4. Modify the title and description fields as desired.

Tip:

You can also modify the other areas of a selected Replication List while the **Properties** dialog box is open.

5. Click **Replication List Properties** to modify dependency options.
6. Click **Save & Close**.

Note:

Some objects may be dependent on other objects and may not function correctly when replicated unless those other objects exist on the Destination site as well. If you check any of the supported dependency options, Federation replicates these objects even if they are not added to the Replication List. For more information, see [Creating Replication Lists](#).

To modify objects in a Replication List

1. Go to the **Replication Lists** area of the **CMC**.
2. Select a **Replication List** to modify its objects.
3. On the **Actions** menu, click **Manage Replication List**.
The **Manage Replication List** dialog box opens with a list of currently added objects.
4. Add or remove objects as desired.

Tip:

You can also modify the other areas of a selected Replication List while the **Manage Replication List** dialog box is open.

Managing Remote Connections

Remote Connection objects contain the information needed to connect to a remote BusinessObjects Enterprise deployment.

Note:

The Remote Connection is always treated as the Origin site. The BusinessObjects Enterprise deployment where you create the Remote Connection object is always treated as the Destination site.

To view a Remote Connection

- Go to the **Federation** area of the CMC.
 - Click **Remote Connections** to view a list of remote connection objects grouped by folder
 - Or click **All Remote Connections** to view a flat list of all Remote Connection objects

Creating Remote Connections

A Remote Connection in Federation will connect to a remote BusinessObjects Enterprise 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.

To organize your Remote Connections, you may create folders and subfolders.

To create a Remote Connection folder

1. Go to the **Federation** area of the **CMC**.
2. Click **Remote Connections**.
3. Click **Manage**.
4. Click **New**, and then click **Folder**.

A **Create Folder** dialog box opens.

5. Enter a folder name and click **OK**.

You can now create a Remote Connection by selecting the folder you want it listed in.

To create a new Remote Connection

To connect to a remote BusinessObjects Enterprise deployment, you must create a Remote Connection in Federation.

1. Go to the **Federation** area of the **CMC**.
2. Click **Remote Connections** folder.
3. Click **Manage**.
4. Click **New**, and then click **New Remote Connection**.

The **New Remote Connection** dialog box opens.

5. Enter a title, description and related fields as required:

Note:

All fields are mandatory, except for “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 BusinessObjects Enterprise whether they are the Origin or Destination site, or another deployment. Use this format: <code>http://application_yourserver_machine_name:port/dswsbobje</code> Example: <code>http://mymachine.mydomain.com:8080/dswsbobje</code>

Field	Description
Remote System CMS	The name of the CMS you want to connect to that is accessible through Federation Web Services. This will be treated as the CMS for the Origin site. This is the format: CMS_Name:port (port optional if it is 6400) Example: mymachine:6400
User Name	The user name that will be used to connect to the Origin site. Note: Ensure the account you are using has viewing rights of the Replication List on the Origin site.
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, NT, AD or LDAP.
Cleanup Frequency (in hours)	How often Replication Jobs that use this Remote Connection object should perform an object cleanup. Enter only positive whole numbers. The unit is hours. Default = 24. For more information, see Managing Object Cleanup .
Limit the number of cleanup objects to	The number of objects a Replication Job cleans up. For more information, see Managing Object Cleanup . (Optional)

6. Click **OK**.

Modifying Remote Connections

Once you create a Remote Connection in Federation 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. Select the **Remote Connection** folder and then select the Remote Connection object you want to modify.
4. On the **Manage** menu, click **Properties**.

The **Remote Connections Properties** dialog box opens. You can modify a variety of properties, including the:

- **Title**
- **Description**
- **Remote System Web Service URI**
- **Remote System CMS**
- **User Name**
- **Password**
- **Cleanup Frequency (in hours)**
- **Limit the number of cleanup objects to:**
- **Authentication**

5. Select your changes.
6. Click **Save & Close**.

Managing Replication Jobs

A Replication Job is a type of object that runs on a schedule and is used to replicate content between two BusinessObjects Enterprise deployments in Federation. Each Replication Job must have one Remote Connection, and one Replication List associated with it.



To view a list of your Replication Jobs:

1. Go to the **Federation** area of the **CMC**.
2. Select the **Remote Connection** folder to view a list of **Remote Connections**.
 - Select a **Remote Connection** object to view a list of **Replication Jobs**
 - Or click **All Replication Jobs** to view a list of all **Replication Jobs**

Creating a Replication Job

A Replication Job is an object that is used to replicate content between two BusinessObjects Enterprise deployments in Federation, which runs on a schedule. Each Replication Job must have only one Remote Connection, and one Replication List associated with it.

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: 

To create a Replication Job

1. Go to the **Federation** area of the **CMC**.
2. Click **Remote Connections** folder.
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 proceed further using the wizard.

4. Click **Manage**.
5. Click **New**, and then click **New Replication Job**.
A **New Replication Job** dialog box appears.
6. Enter the **Title** and **Description** of the **Replication Job**.
7. Select **Next**.
A list of available **Replication Lists** on the Origin site appears.
8. Select the desired **Replication List** to use with your **Replication Job**.
9. Click **Next**.
10. Select configuration options as described in table.

Option	Description
1) Enable object clean-up on destination	<p>Forces the Replication Job to delete any replicated objects on the Destination site, where the originating object on the Origin site was removed. For more information, see Managing Object Cleanup.</p> <p>Note: Object Cleanup will not delete objects replicated using dependencies or objects selected on the Replication List.</p>
2a) One-way replication	<p>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.</p>
2b) Two-way replication	<p>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.</p>
3a) Origin site wins	<p>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.</p>
3b) No automatic conflict resolution	<p>Specifies that no action is taken to resolve any detected conflicts. For more information, see Managing conflict detection and resolution.</p>
3c) Destination site wins (only available with two-way replication)	<p>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.</p>

Option	Description
4a) Normal replication	Specifies that the Replication Job acts normally.
4b) 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.
4c) 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.
5a) Replicate all objects (only visible with two-way replication)	Replicates the entire Replication List. Note: This is the most complete option but takes the longest to perform.
5b) 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. For more information, see Remote scheduling and locally run instances .
5c) 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.
5d) Replicate locally run completed instances	Replicates completed instances only from the Destination site to the Origin site. For more information, see Remote scheduling and locally run instances .

11. Click **OK**.

Scheduling a Replication Job

Once you create a Replication Job, you may schedule it to run once or on a recurring basis. You may also schedule multiple Replication Jobs on one Destination site from one Origin site.

Note:

If you schedule multiple Replication Jobs on one Destination site, only one Replication Job can connect to the Origin site at a time. All other Replication Jobs that try to connect will be moved to a pending state and remain pending until they are able to automatically connect to the Origin site.

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**.
4. Click **Schedules**.
5. Select the desired scheduling options.

Modifying a Replication Job

Once you create a Replication Job in Federation, you can modify its properties, scheduling, instances, user rights, and the Replication List it uses.

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. On the **Manage** menu, click **Manage object properties**.
6. View and edit the **Properties**, **Schedule**, **History**, **Replication List**, and **User Security**, as desired.

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.

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. Click the **Federation** area of the **CMC**.
2. Click **All Replication Jobs** folder.
3. Select the desired **Replication Job** from 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 outputted in XML format and uses an XSL form to format the information into an HTML page for viewing.

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:

- Windows:<InstallDir>\BusinessObjects Enterprise 12.0\Logging
- Unix:<InstallDir> /bobje/logging

Example: Accessing a log file

If you are a Windows user and installed BusinessObjects Enterprise to the default location, go to: `C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Logging`

If you want to access the XSL file directly, go to:

- Windows: `<InstallDir> \common\4.0\java\lib\`
- Unix: `<InstallDir>/boobje/java/lib`

If you are a Windows user and installed BusinessObjects Enterprise to the default location, go to: `C:\Program Files\Business Objects\common\4.0\java\lib\`

The name of the XSL file is: `replicationLog.xsl`

The log file is displayed in the language of the user's Product Local that the Replication Job is running under.

Note:

If the language is not installed on the Origin site, its entries default to English. This may result in a log file that contains entries in two languages.

Managing security rights

Security is important when working in any BusinessObjects Enterprise deployment. However, because Federation replicates content between separate deployments and requires collaboration with other administrators, it is necessary to understand how security performs before you begin using Federation.

Administrators in separate deployments must coordinate with each other before enabling Federation. Once content is replicated, administrators can change, modify, and administer content. For these security reasons, it is important that you maintain communication with other administrators.

The following chapter discusses the following features to accomplish certain tasks:

- Rights required on the Origin site
- Rights required on the Destination site

- Rights required on Federation specific objects
- Scenarios that occur in Federation

Tip:

It is recommended that you read this chapter prior to starting Federation.

Rights required on the Origin site

This section describes the actions to the Origin site and the required rights of the user account connecting to the Origin Central Management Server (CMS). This is the account you enter in the Remote Connection object on the Destination site.

Note:

This section only describes the required rights on the Origin Site. For Destination site rights, refer to the following section.

One-way replication

Action: To perform replication only from the Origin site to the Destination site. Minimum rights required:

- “View” and “Replicate” rights on all objects to replicate
- “View” right on the Replication List

Note:

“View” and “Replicate” rights are required on all objects being replicated, including objects that are automatically replicated by dependency calculations.

Two-way replication

Action: To perform replication from the Origin site to the Destination site, and from the Destination site to the Origin site. Minimum rights required:

- “View” and “Replicate” rights on all objects to replicate
- “View” right on the Replication List
- “Modify Rights” on user objects to replicate any password changes

Scheduling

Action: To allow remote scheduling to occur on the Origin site from the Destination site. Minimum rights required:

- “Schedule right for all objects that will be remotely scheduled”

Rights required on the Destination site

This section describes actions 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.

All Objects

Action: To replicate objects regardless of one-way or two-way replication. Minimum rights required:

- “View”, “Add”, “Edit”, “Modify Rights” on all objects
- “Modify User Password” rights in addition to above, for user objects.

First Replication

Action: The first time the Replication Job is run. This scenario is different than the following scenarios as no objects exist on the Destination site yet. Therefore, the user account the Replication Job is running under must have specific rights at all the top level folders and default objects that will have content added to them. Minimum rights required:

- “View”, “Add”, “Edit”, “Modify Rights” on all top level folders.

Federation specific objects

This section details scenarios that are specific to Federation that you may encounter.

Object Cleanup

Object Cleanup only occurs on the Destination site.

Action: To delete objects on the Destination site. Minimum rights required:

- “Delete” rights for the account that the Replication Job is running under on all objects that may be potentially deleted

Enabling 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.

To safeguard against undesired changes being sent to the Origin site:

- Deny “Edit” rights of the user account used to connect in the Remote Connection Object

Note:

For Remote Scheduling, you may 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 sent back to the Origin site, and changes made on the Origin site are sent to the Destination site.

Disabling 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.

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.

To disable clean up on certain objects:

- Deny “Delete” rights of the user account the Replication Job is running under on the objects you wish to keep.

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 only have the “View” rights for Group A associated with it.

Note:

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 can't 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 its log file, which shows the object referenced the unreplicated object and dropped its reference.

Security on an object for a particular user or group is only replicated from the Origin site to the Destination site. You may set security on replicated objects on the Destination site, but those settings will not be replicated to the Origin site.

Replicating security on an object using access levels

Similar to the previous section, rights must be defined by access levels to remain. 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 a imported object. This option is available on the Replication List.

Note:

Default access levels are not replicated, but references will be maintained.

Replicating third-party users and groups

In Federation you can replicate third-party users and groups, specifically NT, 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

First: map the users and groups on the Origin site for Federation to replicate them properly. Second: replicate the mapped users and groups to the Destination site.

Note:

Do not map groups and users separately on the Destination site. If you do, they will have different unique identifiers (CUIDs) on the Destination and Origin sites, and Federation will not be able to match the user or groups.

Example:

The administrator maps Group A with User A on the Origin and Destination sites. Both Group A and User A have different unique identifiers on the Origin and Destination sites. During replication, Federation cannot match them and Group A or User A are not replicated due to an alias conflict.

Note:

- The destination site should be set up to use NT, AD or LDAP authentication before you attempt to replicate third-party users and groups.
- After replicating an AD or LDAP group for the first time, users in this group are not be able 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**.

- 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 NT, 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. It will have different CUIDs and Federation won't be able to replicate them properly.

Note:

It is important to create the account on one site and then replicate it to the other.

Replicating universes and universe connections

When using Federation to replicate Universes between BusinessObjects Enterprise deployments, it is important to take the time to plan what the desired results should be. A Universe object will not function without an underlying Universe Connection; a Universe object must have a relationship to an existing, functioning Universe Connection in order to work properly.

Universe Connection objects contain information required to connect to a reporting database. In order to function properly, the information they contain needs to be valid and allow a database connection to be established.

To ensure that dependent Universe Connections are replicated with the Universes, when you create or modify the replication list that contains the Universes always choose the **Include connections used by selected universes** and **Include universes required by selected universes** options.

The following two examples demonstrate the process of replicating Universes and their related Universe Connections.

Note:

- If you are using Two-Way replication and replicate a Universe from the Origin without its Universe Connection to the Destination, in subsequent

replications the Origin's Universe may have its relationship to the Universe Connection on the Origin overwritten or removed. To avoid, always replicate the Universe Connections with the Universes.

- 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.

Example:

When replicating Universes and Universe Connections, you must ensure that the connectivity environment on the Origin matches the connectivity environment on the Destination.

For example, if the Universe Connection uses an ODBC connection called "TestODBC", then there needs to be an ODBC connection called "TestODBC" on the Destination environment that works. 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 schema's of the databases must be the same.

Example:

If you want the replicated Universe on the Destination to use a different database then what the Universe on the Origin uses, replicate the Universe Connection, but have the Destination connectivity information on the machine point to the desired database.

For example, if the Universe Connection on the Origin is using an ODBC connection called "Test" pointing to "DatabaseA", have an ODBC connection on the Destination also called "Test" but pointing to "DatabaseB".

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.

How to use Object Cleanup

Separate Replication Jobs that use the same Remote Connection work together during Object Cleanup. This means that your Replication Job will clean up objects within its Replication List, as well as objects within other Replication Lists that use the same Remote Connection. A remote connection is only considered the same if the parent of the Replication Job is the same remote connection object.

Example:

Replication Jobs A and B replicate Object A and Object B. They both replicate from the same Origin site and use the same Remote Connection. If the Origin site deletes Object B, Replication Job A will see that Object B was deleted. Even though Replication Job B is the one replicating it, Object B will also be removed from the Destination site. When Replication Job B executes it won't need to run an Object Cleanup.

Note:

Only objects on the Destination site are deleted during Object Cleanup. If you remove an object from the Origin site that is part of a replication, the object will be removed from the Destination site. However, if an object is removed from the Destination site, it will not be removed from the Origin site during Object Cleanup, even if the replication job is in two-way replication mode.

Objects that are deleted or removed from the Replication List are not deleted from Destination site. To properly remove an object that is specified explicitly on 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.

Object Cleanup limits

In the Remote Connection object, you can define the number of objects a Replication Job will clean up at one time. Federation automatically tracks where the clean up job ends. This way, the next time you run a Replication Job, it starts the next clean up job at that point.

Tip:

To complete a Replication Job faster, limit the number of objects for cleanup.

Example:

Replication Jobs A and B are replicating Object A and Object B. Both objects are replicated from the same Origin site and use the same Remote Connection.

If the Origin site deletes Object B and the object limit is set to 1, the next time Replication Job A runs, it will only check if Object A has been deleted. This way, the Object B is not checked and will not be deleted.

Next, Replication Job B runs and starts the object cleanup at the point where Replication Job A ended. It will check if Object B has been deleted and remove it from the Destination site. You can find this option on the Remote Connection object's property "Limit the number of clean up objects to:"

Note:

If you do not select this option, all Replication Jobs that use this Remote Connection will check all objects for potential clean up.

Object Cleanup frequency

You can set the how often a Replication Job performs object cleanup in the Remote Connection "Cleanup Frequency" field.

Note:

You must enter a positive whole number, which represents the number of hours to wait between object cleanup processing.

Example:

Replication Jobs A and B replicate Object A and Object B. Both objects are replicated from the same Origin site and use the same Remote Connection.

If Object B is deleted from the Origin site + the Object Limit is set to 1 + the Cleanup Frequency is set to 150 hours + Replication Job A runs next, it will check if Object A has been deleted. Because the Object limit is set to 1, Object B will not be checked or deleted.

The next cleanup occurs 150 hours after Replication Job A did the initial check. Although Replication Jobs A and B may execute many times before the 150 hour limit, neither will attempt to run an Object Cleanup. After 150 hours, the next Replication Job will execute and attempt cleanup. Then it will determine that Object B was deleted, and then delete it.

Enabling and disabling options

Each Replication Job can participate in Object Cleanup. Use “Enable Object Cleanup on destination” option on a Replication Job to instruct it whether to run an Object Cleanup. In some cases, you may have high priority Replication Jobs you do not want to participate in Object Cleanup, so you can execute them as quickly as possible. To do this, disable Object Cleanup.

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, or refresh from destination.

One-way replication

With one-way replication, you can only replicate content in 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 BusinessObjects Enterprise deployment where objects are created, modified and administered. Other BusinessObjects Enterprise 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

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 sent to Destination sites, and changes made on a Destination site are sent to the Origin site during replication.

Note:

To perform remote scheduling and to send locally run instances back to the Origin site, you must select two-way replication mode.

If you have multiple BusinessObjects Enterprise 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

For more information, see [Remote scheduling and locally run instances](#).

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 executes.

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. That's why "Refresh from origin" and "Refresh from destination" 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 highlight scenarios using "Refresh from Origin" and "Refresh from Destination" where certain objects will be missed due to the optimization.

Scenario 1: The addition of the 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 Import Wizard or the BIAR command line.

When you add objects to an area that is being replicated using Import Wizard 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 Import Wizard or BIAR command line.

Note:

After importing new objects into an area that is being replicated on the Origin site, it is recommended that you execute 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 execute 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 may replicate content quickly.

Note:

This scenario can be costly for large Replication lists, so it is recommended that you do not use this option often. For example, it is not necessary to create replication jobs to refresh from the Origin to Destination mode on an hourly schedule. These modes should be used in “run now” or infrequent schedules.

Note:

In some cases, you cannot use conflict resolution, including: “Refresh from origin”: destination site option wins is blocked, or “Refresh from destination”: origin wins option is blocked.

Managing conflict detection and resolution

In Federation, a conflict occurs 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.

Example: Two types of object conflicts

1. If Frank modifies the report file on the Origin site, and Simon modifies the replicated version on the Destination site.
2. If Abdul modifies the name of a report on the Origin site, and Maria modifies the name of the replicated report on the Destination site.

Some instances do not create a conflict. For example, if Lily modifies the name of a report on the Origin site, and Malik modifies the description of the replicated version on the Destination site, the changes merge together.

One-way replication conflict resolution

In one-way replication, you have two choices for conflict resolution:

- “Origin site takes precedence”
- “No automatic 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.

Example:

Frank changes the name of a report to Report A. Simon changes 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.


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.

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 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, as shown here:

- If there is a conflict, objects will be flagged with a conflict icon, as shown

in this example:  . A warning message also appears in the “Properties” page.

Note:

The list is updated when a Replication Job that uses a Remote Connection is completed. It contains all objects in conflict for all of the Replication Jobs that use its specific Remote Connection.

Note:

Any user with access to the CMC and the Replication Job instances can access the XML log outputted 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.

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.
- 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, as shown here:  If there is a conflict, objects will be flagged with a conflict icon as shown here:



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 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 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 may delete the object on the Destination site.

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 BusinessObjects Enterprise 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, it is recommended that you enable file caching in Federation.

Session variable

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\Business  
Objects\Tomcat55\webapps\dswsbobje\WEB-INF\classes
```

To activate 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.

File caching

File caching allows Web Services to handle very large attachments without buffering them in memory. If it is not enabled during large transfer sizes, all

of the Java's Virtual Machine memory can be utilized and replication may fail.

Note:

File caching decreases performance as the Web Services process to files instead of memory. You may use a combination of both options and send large transfers to a file and smaller ones into memory.

To enable file caching, modify the `Axis2.xml` located at:

```
<App Server Installation  
Directory>\dswsbobje\Web-Inf\conf
```

For example:

```
C:\Program Files\Business  
Objects\Tomcat55\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.

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.

BusinessObjects Enterprise Web Services are located in:

```
<App Server Installation  
Directory>\dswsbobje\WEB-INF\services
```

Example:

C:\Program Files\Business Objects\Tomcat55\webapps\dswebobje\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:

`services.xml` file is located in:

C:\Program Files\Business Objects\Tomcat55\webapps\dswebobje\WEB-INF\services\federator\META-INF

Change service name from:

`<service name="Federator">`

To:

`<service name="Federator" activate="false">`

Remote scheduling and locally run instances

This section details Remote Scheduling, Locally Run Instances and Instance Share. These features allow reports to run where the data resides and send completed instances to the appropriate locations.

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 runs, it uses the completed instance to update the copy on the Destination site. Once updated, the instance on the Destination site is complete.

Note:

A Replication Job has to run twice in order to bring back one completed instance.

Example:

1. Tom schedules Report A for Remote Scheduling.
2. Report A is created on the Destination site and is in the pending state.
3. Replication Job A runs. First: it replicates changes from the Origin site to Destination site (including previously completed instances). Second: it copies the instance in the pending state to the Origin site, as well as changes to be replicated from the Destination site to the Origin site.
4. At the Origin site, the scheduler picks up the instance in the pending state and sends it to the appropriate job server for processing. The instance is then processed and placed in the completed state on the Origin site.
5. Replication Job A runs again. When it replicates content from the Origin site to the Destination site, the completed instance Report A is picked up and changes are applied to the Destination's version.
6. Once this task is done, the Destination's version is complete.

Remote Scheduling only works with a two-way Replication Job. You must enable "Replicate remote schedules". This option is located on the Replication Job Properties page in the "Replication Filters" area. In some scenarios, you may want to replicate remotely scheduled jobs more frequently than other objects on your Replication List. To do this, create two Replication Jobs.

Enable one job with “Replicate remote schedules” for a Replication Job that is only focusing on Remote Scheduling. Enable the other job with “Replicate document templates” or “Replicate all objects (no filter)”.

Note:

When you enable Remote Scheduling, completed and failed instances appear on both the Origin and Destination site.

If a user on the Destination site schedules a report for Remote Scheduling and the user does not exist on the Origin site, the instance will fail on the Origin site. The owner of the failed instance will be the user account of the Remote Connection object used to connect to the Origin.

A Replication Job may only be configured for Remote Scheduling, but it always replicates the ancestor objects of the report instance. This means that if there are any changes between replications, it replicates the actual report, reports folder, and so on. If you do not want these changes on the Destination site to be replicated to the Origin site, see [Managing security rights](#).

Locally run instances

Locally Run Instances are instances of a report that are processed from reports on the Destination site. With Federation, you can replicate the completed instances from the Destination site to the Origin site.

To enable a Replication Job to replicate completed and failed instances from the Destination site to the Origin site, click **Replication Job Properties > Replication Filters > Replicate locally run completed instances**.

In some cases, you may want a Replication Job to only replicate locally run instances. To do this, enable “Replicate locally run completed instances”.

Note:

When you enable Locally Run Instances on a Replication Job, both completed and failed instances are replicated to the Origin site. This means that there will be copies on both the Origin and Destination sites.

Pending instances are never replicated.

If the owner of a locally run instance does not exist on the Origin site, then the owner will be the user account used to connect in the Remote Connection object.

Instance share

When you enable Remote Scheduling and Locally Run Instances in a Replication Job, instance share may occur if one Origin site with multiple Destination sites are replicating the same report.

Example:

Report A originates on the Origin Site, while Destination sites A and B are replicating it. Instance share occurs at both Destination sites:

- Enabled Replication Jobs with “Replicate remote schedules” and/or “Replicate locally run completed instances” Replicate Report A with the same Replication Job as above
- Schedule Report A on the Destination site to “run at origin” and/or to run locally

If both Destination sites A and B replicate Report A and their corresponding Replication Jobs are replicating remote schedules and/or replicating locally run instances, then any instances that were processed at Destination site A and/or at the Origin site on behalf of Destination site A will be shared with Destination site B.

Similarly, any instances processed at Destination site B and/or processed at the Origin site will also be shared with Destination site A. Finally, the Origin site and Destination sites A and B will have an identical set of instances.

Instance share is ideal in many cases. For example, when users from other sites need to access information from their sister deployments. In this case, to prevent instances from being viewed by users at the local site, ensure the proper security rights are set. For example, in a report object, apply the rights so users can see only the instances they own.

Note:

All objects follow the BusinessObjects Enterprise 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. For more information, see [Managing security rights](#).

Importing and promoting replicated content

In some cases, you may choose to import or promote replicated content from one BusinessObjects Enterprise system to another. This section discusses these features in Federation.

Note:

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

Importing replicated content

If you use the Import Wizard to import content from one BusinessObjects Enterprise deployment to another, the Import Wizard 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:

BusinessObjects Enterprise System A is a Destination Site in a Federation process. Report A, a replicated report on System A, is imported from System A to BusinessObjects Enterprise System B using the Import Wizard.

Outcome: When Report A is copied to System 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 System A, it will not be in conflict on System B. Essentially it is treated as an object that originated from System B.

Note:

The CUID may or may not be the same, depending on the import choices you select in the Import Wizard.

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 Import Wizard.
- Ensure the first Replication Job either has conflict resolution set to "Origin wins" or "Destination wins".

Tip:

Instead of importing the object using Import Wizard 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 BusinessObjects Enterprise System A. System X used Federation to replicate Report A from System A to System X. The Import Wizard then imported Report A from System X to System Y.

Plan: System Y wants to set up Federation to System A, and keep Report A as part of Replication. System Y is the Destination and System A is the Origin.

Action: When importing Report A from System X to System Y, the CUID of Report A must be preserved. In addition, when the first Replication Job executes, it will try to replicate Report A. Because the object already exists on System Y, replication will produce a conflict. To specify which version to use, you must set the Conflict Resolution mode to either "Origin wins" or "Destination wins".

Note:

In this example, it is recommended that instead of importing the object using Import Wizard 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 Import Wizard to import from System X to System Y.

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 BusinessObjects Enterprise 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 Import Wizard to promote your content from your Origin site in the testing environment to the machine in Production that will act as your Origin site.

Note:

The Replication List object is not selectable when using the Import Wizard.

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 Import Wizard 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.

Re-pointing a destination site

Currently, once an object is replicated from an Origin site, it must always be replicated from that Origin site and can't be replicated from another BusinessObjects Enterprise system. Even if the Remote Connection object is edited to point to a new BusinessObjects Enterprise system, any attempt

to replicate an object that was replicated from a different BusinessObjects Enterprise 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:

Once you copy a replicated object, the CUID of the copy is changed and the copy will not contain any replication information.

Best practices

With Federation, it is possible to optimize the performance of a Replication Job if you follow the configuration steps described in this section.

If there a large number of objects in a single Replication Job, you can take additional steps to ensure success when you run the Replication Job. Typically, you should be able to replicate up to 32,000 objects in each Replication Job. However, some deployments may need to make configurations with smaller or larger replication sizes. If you experience problems, refer to [Troubleshooting error messages](#).

Note:

It is recommended that you read [Using Web Services in Federation](#) before you begin the following steps.

1) Obtain a dedicated Web Services provider

In Federation, replicated content is sent via Web Services. In a default installation of BusinessObjects Enterprise, all Web Services utilize the same web service provider. This means that larger Replication Jobs may tie up 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 BusinessObjects Installer and install BusinessObjects Enterprise 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 the BusinessObjects Web Services and Tomcat. To do this, launch

Installer on the desired machine, select “Custom Install” and select either the “Web Tier Components” option or “BusinessObjects Web Services”.

Note:

- You must input an existing CMS, for example the hostname, port, and administrator password.
- 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 BusinessObjects Enterprise and Tomcat, the default available memory is 1 GB. To increase the available memory for Tomcat:

In Windows:

1. Open the **Tomcat Configuration**. Click **Start > Programs > Tomcat > Tomcat Configuration**.
2. Select **Java**.
3. In the **Java Options** text 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 "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for Tomcat
JAVA_OPTS="-Dboj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" -o "$SOFTWARE" = "HP-
UX" ];
then
```

```

JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"

fi
export JAVA_OPTS
# fi

```

3. Increase the `-Xmx1024m` parameter to the desired size.

Example:

To increase the memory to 2 GB, enter: `-Xmx2048m`

Tip:

For other Java application servers, refer to your Java application server's documentation to increase the available memory.

3) Reduce the size of the BIAR files being created.

Federation uses Web Services to replicate content between the Origin site and Destination site. Objects are grouped together and compressed into BIAR files for more efficient transportation.

When replicating a large number of objects, configure your Java Application Server to create smaller BIAR files. Federation will package and compress objects across multiple smaller BIAR files so the number of objects you want to replicate will not be limited.

To reduce the size of the BIAR files created, add the following Java parameters to your java application server:

```

Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit

```

`bobj.biar.suggestSplit` suggests an appropriate size of the BIAR file, which it will try to meet. Suggested new value is 90MB.

`bobj.biar.forceSplit` will force a BIAR file to stop at a given size. Suggested new value is 100 MB.

Note:

You do not need to change the default BIAR file size settings unless your application server is running out of memory and its maximum heap size (see [Current release limitations](#)) cannot be increased any further.

For Tomcat Windows:

1. Open the **Tomcat Configuration** tool. Click **Start > Programs > Tomcat > Tomcat Configuration**.
2. Select **Java**.
3. Under the **Java Options** text 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}enter  
prisel20 -Djava.awt.headless=true"  
  
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o  
"$SOFTWARE" = "Linux" -o "$SOFTWARE" = "HP-UX" ]; 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>`

Current release limitations

Federation is a very flexible tool, however certain limitations may effect 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 BusinessObjects Enterprise 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 BusinessObjects Enterprise deployment on the site where the user resides.

- Business Views and associated objects

BusinessObjects Enterprise 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

BusinessObjects Enterprise 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. For more information, see [Managing Object Cleanup](#).

- 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.

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 ASX0OFyvy0fJnRcD0dzNTZg (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. For more details, see [Current release limitations](#).

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. For more details, see [Current release limitations](#).

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. For more details, see [Best practices](#).

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. For more details, see [Best practices](#).

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:MaxPermSize=256m"`.
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 processDFCCommands 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.



Working with Firewalls



chapter



Understanding communication between BusinessObjects Enterprise components

If your BusinessObjects Enterprise system is deployed entirely on the same subnet, there is no need to perform any special configuration of your firewalls. However, you might choose to deploy some Business Objects components on different subnets separated by one or more firewalls.

It is important to understand the communication between BusinessObjects Enterprise servers, rich clients, and the web application server hosting the BusinessObjects Enterprise SDK before configuring your BusinessObjects Enterprise system to work with firewalls.

Related Topics

- [Configuring BusinessObjects Enterprise for firewalls](#)
- [Examples of typical firewall scenarios](#)

Overview of BusinessObjects Enterprise servers and communication ports

It is important to understand BusinessObjects Enterprise servers and their communication ports if the BusinessObjects Enterprise system is deployed with firewalls.

Each BusinessObjects Enterprise server binds to a Request Port

A BusinessObjects Enterprise server, such as the Input File Repository Server, binds to a Request Port when it starts. Other BusinessObjects Enterprise components including BusinessObjects Enterprise servers, Business Objects rich clients, and the Business Objects SDK hosted in the web application server can use this Request Port to communicate with the server.

A server will select its Request Port number dynamically unless it is configured with a specific port number. A specific Request Port number must be configured for servers that communicate with other BusinessObjects Enterprise components across a firewall.

Each BusinessObjects Enterprise server registers with the CMS

BusinessObjects Enterprise servers register with the CMS when they start. When a server registers, the CMS records:

- The hostname (or IP address) of the server's host machine.
- The server's Request Port number.

The Central Management Server (CMS) uses two ports

The CMS uses two ports: the Request Port and the Name Server Port. The Request Port is selected dynamically by default. The Name Server Port is 6400 by default.

Other BusinessObjects Enterprise servers will initially contact the CMS on its Name Server port. The CMS will respond to this initial contact by returning the value of its Request Port. The Business Objects servers will use this Request Port for subsequent communication with the CMS.

The Central Management Server (CMS) provides a directory of registered servers

The CMS provides a directory of the BusinessObjects Enterprise servers that have registered with it. Other BusinessObjects Enterprise components such as BusinessObjects Enterprise servers, Business Objects rich clients, and the Business Objects SDK hosted in the web application server can contact the CMS and request a reference to a particular server. A server's reference contains the server's Request Port number and the host name (or IP address) of the server's host machine.

BusinessObjects Enterprise components might reside on a different subnet than the server they are using. The host name (or IP address) contained in the server reference must be routable from the component's machine.

Note:

The reference to a BusinessObjects Enterprise server will contain the server machine's host name by default. (If a machine has more than one hostname, the primary hostname is chose). You can configure a server so that its reference contains the IP address instead.

Related Topics

- [Communication between BusinessObjects Enterprise components](#)

Server Intelligence Agents (SIA) communicate with the Central Management Server (CMS)

Your deployment will not work if the Server Intelligence Agent (SIA) and Central Management Server (CMS) cannot communicate with each other. Ensure that your firewall ports are configured to allow communication between the SIA and the CMS.

Job server child processes communicate with the data tier and the CMS

Most job servers create a child process to handle a task such as generating a report. The job server will create one or more child processes. Each child process has its own Request Port.

By default, a job server will dynamically select a Request Port for each child process. You can specify a range of port numbers that the job server can select from.

All child processes communicate with the CMS. If this communication crosses a firewall, you must:

- Specify the range of port numbers that the job server can select from. Note that the port range should be large enough to allow the maximum number of child process as specified by `-maxJobs`.
- Open the specified port range on the firewall.

Many child processes communicate with the data tier. For example, a child process might connect to a reporting database, extract data, and calculate values for a report. If the job server child process communicates with the data tier across a firewall, you must:

- Open a communicate path on the firewall from any port on the job server machine to the database listen port on the database server machine.

Related Topics

- [Job servers](#)

Communication between BusinessObjects Enterprise components

BusinessObjects Enterprise components, such as browser clients, rich clients, servers, and the BusinessObjects Enterprise SDK hosted in the web application server, communicate with each other across the network during typical workflows. You must understand these workflows to deploy Business Objects products across different subnets that are separated by a firewall.

Requirements for communication between BusinessObjects Enterprise components

Deployments of BusinessObjects Enterprise must conform to these general requirements.

1. Every BusinessObjects Enterprise server must be able to initiate communication with every other BusinessObjects Enterprise server on that server's Request Port.
2. The CMS uses two ports. Every BusinessObjects Enterprise server, BusinessObjects Enterprise rich client, and the web application server that hosts the BusinessObjects Enterprise SDK must be able to initiate communication with the Central Management Server (CMS) on both of its ports.
3. Every job server child process must be able to initiate communication with the CMS on both of its ports.
4. Rich clients must be able to initiate communication with the Request Port of the Input and Output File Repository Servers
5. If Desktop Intelligence and Web Intelligence rich clients use Auditing, they must be able to initiate communication with the Request Port of the Adaptive Processing Servers that hosts the Client Auditing Proxy Service.
6. In general, the web application server that hosts the BusinessObjects Enterprise SDK must be able to initiate communication with the Request Port of every BusinessObjects Enterprise server.

Note:

The web application server only needs to communicate with BusinessObjects Enterprise servers that are used in the deployment. For example, if Crystal Reports is not being used, the web application server

does not need to communicate with the Crystal Reports Processing Servers.

7. Job Servers use the port numbers that are specified with the `-requestJSChildPorts <port range>` command. If no numbers are specified in the command line, the servers use random port numbers. To allow a job server to communicate with an FTP or mail server on another machine either open all of the ports in the range specified by `-requestJSChildPorts` on your firewall, or add the job server child process as an exception for your firewall.
8. The CMS must be able to initiate communication with the CMS database listen port.
9. The Connection Server, most Job Server child process, and every Processing Server must be able to initiate communication with the reporting database listen port. Each database vendor uses a different listen port. To find the default listen port number, see your database documentation.

Related Topics

- [BusinessObjects Enterprise port requirements](#)

BusinessObjects Enterprise port requirements

This section lists the communication ports used by BusinessObjects Enterprise servers, BusinessObjects Enterprise rich clients, the web application server hosting the BusinessObjects Enterprise SDK, and third-party software applications. If you deploy BusinessObjects Enterprise with firewalls, you can use this information to open the minimum number of ports in those firewalls.

Port Requirements for Business Objects Applications

This table lists the servers and port numbers used by BusinessObjects Enterprise applications.

Product	Client Application	Associated Servers	Server Port Requirements
Crystal Reports	Crystal Reports Designer	CMS Input FRS Output FRS Report Application Server (RAS) Crystal Reports Cache Server Crystal Reports Page Server Web Intelligence Processing Server	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port RAS Request Port Crystal Reports Cache Server Request Port Crystal Reports Page Server Request Port Web Intelligence Processing Server Request Port

Product	Client Application	Associated Servers	Server Port Requirements
Live Office web application	Live Office	CMS Input FRS Output FRS Report Application Server (RAS) Web Intelligence Processing Server Adaptive Processing Server Crystal Reports Cache Server	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port RAS Request Port Web Intelligence Processing Server Request Port Adaptive Processing Server Request Port Crystal Reports Cache Server Request Port
Live Office Rich Client	Live Office	web application server that hosts the Live Office web application	HTTP port (80 by default)
Business Objects Enterprise	Web Intelligence Rich Client	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port

Product	Client Application	Associated Servers	Server Port Requirements
Business Objects Enterprise	Desktop Intelligence	CMS Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port
Business Objects Enterprise	Universe Designer	CMS Input FRS Connection Server	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Connection Server port
Business Objects Enterprise	Business View Manager	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port

Product	Client Application	Associated Servers	Server Port Requirements
Business Objects Enterprise	Central Configuration Manager (CCM)	CMS Server Intelligence Agent (SIA)	<p>The following ports must be open to allow CCM to manage remote BusinessObjects Enterprise servers:</p> <p>CMS Name Server Port (6400 by default)</p> <p>CMS Request Port</p> <p>The following ports must be open to allow CCM to manage remote SIA processes:</p> <p>Microsoft Directory Services (TCP port 445)</p> <p>NetBIOS Session Service (TCP port 139)</p> <p>NetBIOS Datagram Service (UDP port 138)</p> <p>NetBIOS Name Service (UDP port 137)</p> <p>DNS (TCP/UDP port 53)</p> <p>(Note that some ports listed above may not be required. Consult your Windows administrator).</p>

Product	Client Application	Associated Servers	Server Port Requirements
Business Objects Enterprise	Server Intelligence Agent (SIA)	Every Business Objects server including the CMS	SIA Request Port (6410 by default) CMS Name Server Port (6400 by default) CMS Request Port Request Port for each server that is managed by the SIA
Business Objects Enterprise	Import Wizard	CMS Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port
Business Objects Enterprise	Publishing Wizard	CMS Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port
Business Objects Enterprise	Report Conversion Tool	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port

Product	Client Application	Associated Servers	Server Port Requirements
Business Objects Enterprise	Business Objects Enterprise SDK hosted in the web application server	<p>All Business Objects Enterprise servers required by the deployed products.</p> <p>For example, communication with the Crystal Reports Cache Server Request Port is required only if Crystal Reports is deployed and used.</p>	<p>CMS Name Server Port (6400 by default)</p> <p>CMS Request Port</p> <p>Request Port for each server that is required.</p>
Voyager	OLAP	<p>CMS</p> <p>Multidimensional Analysis Server (MDAS)</p> <p>Input FRS</p> <p>Output FRS</p>	<p>CMS Name Server Port (6400 by default)</p> <p>CMS Request Port</p> <p>MDAS port</p> <p>Input FRS Request Port</p> <p>Output FRS Request Port</p>

Note:

To configure the Report Application Server in a firewalled environment, you must implement the following steps:

1. Open the incoming RAS request port; this port is identified by the `-requestport` server command line switch.
2. Open all outgoing ports:
By default, the RAS server picks a dynamic outgoing port. If you want to limit the outgoing ports, update the following registry keys with your specified range of ports, and enable these ports and the RAS request port.

For Windows, specify the range of ports in the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\CER\RequestPortLower
- HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\CER\RequestPortUpper

For UNIX, specify the range of ports in the following file:

```
<INSTALLDIR>/bobje/data/.bobj/registry/software/business objects/suite 12.0/cer/.registry
```

- "RequestPortLower"=dword:0
"RequestPortUpper"=dword:10000

Port Requirements for Third-Party Applications

This table lists third-party software used by Business Objects products. It includes specific examples from some software vendors, but different vendors will have different port requirements.

Third-party application	Business Objects component that uses the third-party product	Third-party application port requirement	Description
CMS Database	Central Management Server (CMS)	Database server listen port. See the database provider documentation for the default port number.	The CMS is the only server that communicates with the CMS database.

Third-party application	Business Objects component that uses the third-party product	Third-party application port requirement	Description
Reporting Database	Connection Server Every Job Server child process Every Processing Server	Database server listen port. See the database provider documentation for the default port number.	These servers retrieve information from the reporting database.
web application server	Live Office Rich Client All Business Objects portals including InfoView and CMC	HTTP port and HTTPS port. For example, on Tomcat the default HTTP port is 8080 and the default HTTPS port is 443.	The HTTPS port is only required if secure HTTP communication is used.
FTP server	Every Job Server	FTP In (port 21) FTP Out (port 22)	The Job Servers use the FTP ports to allow send to FTP.
Email server	Every Job Server	SMTP (port 25)	The Job Servers use the SMTP port to allow send to email .

Third-party application	Business Objects component that uses the third-party product	Third-party application port requirement	Description
Unix servers to which the Job Servers can send content	Every Job Server	rexec out (port 512) (Unix only) rsh out (port 514)	(Unix only) The Job Servers use these ports to allow send to disk .
Authentication Server	CMS web application server that hosts the BusinessObjects Enterprise SDK every Rich Client, except Live Office and Desktop Intelligence in three-tier "Zabo" mode	Connection port for third-party authentication. For example, the connection server for the Oracle LDAP server is defined by the user in the file ldap.ora.	User credentials are stored in the third-party authentication server. The CMS, BusinessObjects Enterprise SDK, and the Rich clients listed here need to communicate with the third-party authentication sever when a user logs on.

Configuring BusinessObjects Enterprise for firewalls

This section gives step-by-step instructions for configuring your BusinessObjects Enterprise system to work in a firewalled environment.

To configure the system for firewalls

1. Determine which BusinessObjects Enterprise servers must communicate across a firewall. See [Communication between BusinessObjects Enterprise components](#).
2. Configure the Request Port for each BusinessObjects Enterprise server that must communicate across a firewall. See [Configuring port numbers](#).
3. Configure a port range for any Job Server children that must communicate across a firewall. See [Job servers](#).
4. Configure the firewall to allow communication to the Request Ports on the BusinessObjects Enterprise servers that you configured in the previous step. See [Specifying the firewall rules](#).
5. (Optional) Configure the hosts file on each machine that hosts a BusinessObjects Enterprise server that must communicate across a firewall. See [Configure the hosts file for firewalls that use NAT](#).

Specifying the firewall rules

You must configure the firewall to allow the necessary traffic between Business Objects components. Consult your firewall documentation for details of how to specify these rules.

Specify one inbound access rule for each communication path that crosses the firewall. You might not need to specify an access rule for every Business Objects server behind the firewall.

Use the port number you specify in the server **Port** text box. Remember that each server on a machine must use a unique port number. Some Business Objects servers use more than one port.

Note:

If BusinessObjects Enterprise is deployed across firewalls that use NAT, every BusinessObjects Enterprise server on all machines needs a unique Request Port number. That is, no two servers in the entire deployment can share the same Request Port.

Note:

You do not need to specify any outbound access rules. BusinessObjects Enterprise servers do not initiate communication to the web application server, or to any client applications.

Example:

This example shows the inbound access rules for a firewall between the web application server and the BusinessObjects Enterprise servers. In this case you would open two ports for the CMS, one port for the Input File Repository Server (FRS), and one port for the Output FRS. The Request Port numbers are the port numbers you specify in the **Port** text box in the CMC configuration page for a server.

Source Computer	Port	Destination Computer	Port	Action
web application server	Any	CMS	6400	Allow
web application server	Any	CMS	<Request Port number>	Allow
web application server	Any	Input FRS	<Request Port number>	Allow
web application server	Any	Output FRS	<Request Port number>	Allow
Any	Any	CMS	Any	Reject
Any	Any	Other BusinessObjects Enterprise servers	Any	Reject

Related Topics

- [Communication between BusinessObjects Enterprise components](#)

Configure the hosts file for firewalls that use NAT

This step is required only if the BusinessObjects Enterprise servers must communicate across a firewall on which “Network Address Translation ” (“NAT”) is enabled. This step allows the client machines to map a server's hostname to a routable IP address.

This step is required in addition to the steps described in [To configure the system for firewalls](#).

Note:

BusinessObjects Enterprise can be deployed on machines that use Domain Name System (DNS). In this case, the server machine host names can be mapped to externally routable IP address on the DNS server, instead of in each machine's `hosts` file.

Understanding Network Address Translation

A firewall is deployed to protect an internal network from unauthorized access. Firewalls that use “NAT” will map the IP addresses from the internal network to a different address that is used by the external network. This “address translation” improves security by hiding the internal IP addresses from the external network.

BusinessObjects Enterprise components such as servers, rich clients, and the web application server hosting the BusinessObjects Enterprise SDK will use a server reference to contact a server. The server reference contains the hostname of the server's machine. This hostname must be routable from the BusinessObjects Enterprise component's machine. This means the `hosts` file on the BusinessObjects Enterprise component's machine must map the server machine's hostname to the server machine's external IP address. The server machine's external IP address is routable from external side of the firewall, whereas the internal IP address is not.

The procedure for configuring the `hosts` file is different for Windows and UNIX.

To configure the hosts file on Windows

1. Locate every machine that runs a BusinessObjects Enterprise component that must communicate across a firewall on which “Network Address Translation ” (“NAT”) is enabled.
2. On each machine located in the previous step, open the `hosts` file using a text editor like Notepad. The `hosts` file is located at `\WINNT\system32\drivers\etc\hosts`.
3. Follow the instructions in the `hosts` file to add an entry for each machine behind the firewall that is running a BusinessObjects Enterprise server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

To configure the hosts file on UNIX

Note:

Your UNIX operating system must be configured to first consult the “hosts” file to resolve domain names before consulting DNS. Consult your UNIX systems documentation for details.

1. Locate every machine that runs a BusinessObjects Enterprise component that must communicate across a firewall on which “Network Address Translation ” (“NAT”) is enabled.
2. Open the “hosts” file using an editor like `vi`. The `hosts` file is located in the following directory `\etc`
3. Follow the instructions in the `hosts` file to add an entry for each machine behind the firewall that is running a BusinessObjects Enterprise server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

Examples of typical firewall scenarios

This section provides examples of typical firewall deployment scenarios.

Example - Application tier deployed on a separate network

This example shows how to configure a firewall and BusinessObjects Enterprise to work together in a deployment where the firewall separates the web application server from other BusinessObjects Enterprise servers.

In this example, BusinessObjects Enterprise components are deployed across these machines:

- Machine boe_1 hosts the web application server and the BusinessObjects Enterprise SDK.
- Machine boe_2 hosts the Intelligence tier servers, including the Central Management Server, the Input File Repository Server, the Output File Repository Server, and the Event server.
- Machine boe_3 hosts the Processing tier servers, including the Crystal Reports Job Server, the Program Job Server, the Destination Job Server, the List of Values Job Server, the Web Intelligence Job Server, the Web Intelligence Report Server, the Report Application Server, and the Crystal Reports Page Server.

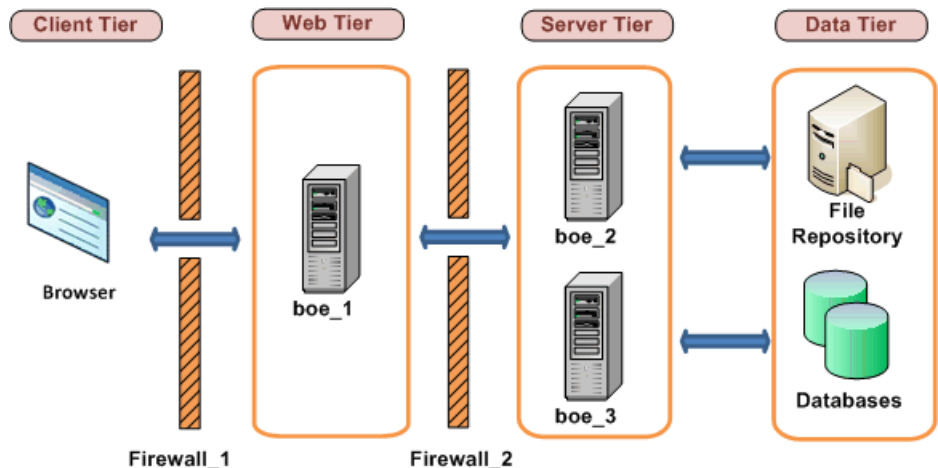


Figure 8-1: Application tier deployed on a separate network

To configure an application tier deployed on a separate network

The following steps explain how to configure this example.

1. These communication requirements apply to this example:
 - The web application server that hosts the BusinessObjects Enterprise SDK must be able to initiate communication with the CMS on both of its ports.
 - The web application server that hosts the BusinessObjects Enterprise SDK must be able to initiate communication with every BusinessObjects Enterprise server.
 - The browser must have access to the http or the https Request Port on the Web Application Server.
2. The web application server must communicate with all Business Objects Enterprise servers on machine boe_2 and boe_3. Configure the port numbers for each server on these machines. Note that you can use any free port between 1,025 and 65,535.

The port numbers chosen for this example are listed in the table:

Server	Port Number
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event server	6425
Crystal Reports Job Server	6435
Program Job Server	6440
Destination Job Server	6445
List of Values Job Server	6450
Web Intelligence Job Server	6455
Web Intelligence Report Server	6460

Server	Port Number
Report Application Server	6465
Crystal Reports Page Server	6470

- Configure the firewalls Firewall_1 and Firewall_2 to allow communication to the fixed ports on the BusinessObjects Enterprise servers and the web application server that you configured in the previous step. Note that port 6400 is the default port number for the CMS Name Server Port and did not need to be explicitly configured.

In this example we are opening the HTTP Port for the Tomcat Application server.

Table 8-5: Configuration for Firewall_1

Port	Destination Computer	Port	Action
Any	boe_1	8080	Allow

Configuration for firewall_2

Source Computer	Port	Destination Computer	Port	Action
boe_1	Any	boe_2	6400	Allow
boe_1	Any	boe_2	6411	Allow
boe_1	Any	boe_2	6415	Allow
boe_1	Any	boe_2	6420	Allow
boe_1	Any	boe_2	6425	Allow
boe_1	Any	boe_3	6435	Allow
boe_1	Any	boe_3	6440	Allow

Source Computer	Port	Destination Computer	Port	Action
boe_1	Any	boe_3	6445	Allow
boe_1	Any	boe_3	6450	Allow
boe_1	Any	boe_3	6455	Allow
boe_1	Any	boe_3	6460	Allow
boe_1	Any	boe_3	6465	Allow
boe_1	Any	boe_3	6470	Allow

4. This firewall is not NAT-enabled, and so we do not have to configure the `hosts` file

Related Topics

- [Configuring port numbers](#)
- [Understanding communication between BusinessObjects Enterprise components](#)

Example - Rich client and database tier separated from BusinessObjects Enterprise servers by a firewall

This example shows how to configure a firewall and BusinessObjects Enterprise to work together in a deployment scenario where:

- One firewall separates a rich client from BusinessObjects Enterprise servers.
- One firewall separates BusinessObjects Enterprise servers from the database tier.

In this example, BusinessObjects Enterprise components are deployed across these machines:

- Machine `boe_1` hosts the Publishing Wizard. Publishing Wizard is a BusinessObjects Enterprise rich client.

- Machine boe_2 hosts the Intelligence tier servers, including the Central Management Server, the Input File Repository Server, the Output File Repository Server, and the Event server.
- Machine boe_3 hosts the Processing tier servers, including: Crystal Reports Job Server, Program Job Server, Destination Job Server, List of Values Job Server, Web Intelligence Job Server, Web Intelligence Report Server, Report Application Server, and the Crystal Reports Page Server.
- Machine Databases hosts the CMS database and the reporting database. Note that you can deploy both databases on the same database server, or you can deploy each database on its own database server. In this example, both the CMS database and the reporting database are deployed on the same database server.

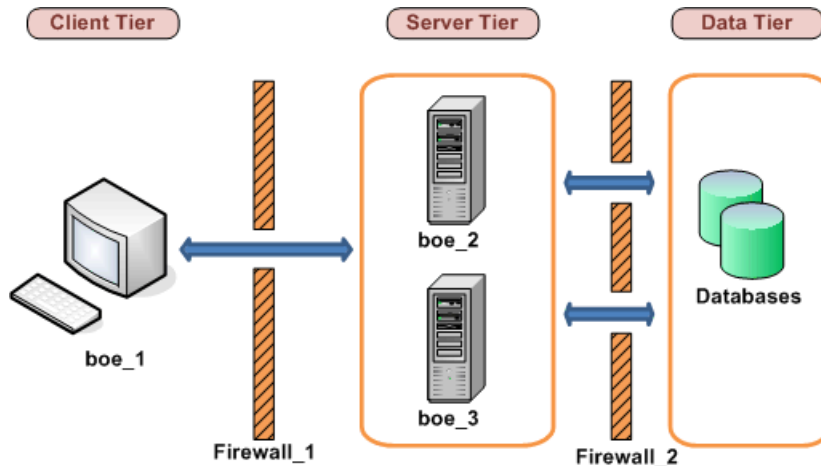


Figure 8-2: Rich client and database tier deployed on separate networks

To configure tiers separated from BusinessObjects Enterprise servers by a firewall

The following steps explain how to configure this example.

1. Apply the following communication requirements to this example:
 - The Publishing Wizard must be able to initiate communication with the CMS on both of its ports.
 - The Publishing Wizard must be able to initiate communication with the Input File Repository Server and the Output File Repository Server.

- The Connection Server, every Job Server child process, and every Processing Server must have access to the listen port on the reporting database server.
 - The CMS must have access to the database listen port on the CMS database server.
2. Configure a specific port for the CMS, the Input FRS, and the Output FRS. Note that you can use any free port between 1,025 and 65,535. The port numbers chosen for this example are listed in the table:

Server	Port Number
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6416

3. We do not need to configure a port range for the Job Server children because the firewall between the job servers and the database servers will be configured to allow any port to initiate communication.
4. Configure *Firewall_1* to allow communication to the fixed ports on the BusinessObjects Enterprise servers that you configured in the previous step. Note that port 6400 is the default port number for the CMS Name Server Port and did not need to be explicitly configured in the previous step.

Port	Destination Computer	Port	Action
Any	boe_2	6400	Allow
Any	boe_2	6411	Allow
Any	boe_2	6415	Allow
Any	boe_2	6416	Allow

Configure *Firewall_2* to allow communication to the database server listen port. The CMS (on boe_2) must have access to the CMS database

and the Job Servers (on boe_3) must have access to the reporting database. Note that we did not have to configure a port range for job server child processes because their communication with the CMS did not cross a firewall.

Source Computer	Port	Destination Computer	Port	Action
boe_2	Any	Databases	3306	Allow
boe_3	Any	Databases	3306	Allow

5. This firewall is not NAT-enabled, and so we do not have to configure the `hosts` file

Related Topics

- [Understanding communication between BusinessObjects Enterprise components](#)
- [Configuring BusinessObjects Enterprise for firewalls](#)



Working with Web Application Container Servers



9

chapter

Web Application Container Server (WACS)

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

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

Web applications such as the CMC are automatically deployed to WACS. WACS does not support deploying Business Objects or external web applications, whether manually or by using wdeploy.

Note:

Business Objects does not support hosting Web Services SDK and QaaWS (DSWS) or Business Process BI (BPBIWS) web services on WACS in this release. Features or applications using web services, such as Live Office or Federation, are also not supported on WACS. Deploying web services to a WACS in a production deployment is not recommended. However, if you want to test unsupported procedures such as adding or removing web services from WACS and configuring single sign-on for Web Services SDK and QaaWS, see the *Web Application Container Server (WACS): Supported and Unsupported Features for BusinessObjects Enterprise XI 3.1* on the Business Objects customer support site: <http://technicalsupport.businessobjects.com>.

Before you start with WACS, it may be helpful to keep these concepts in mind:

- Central Management Console (CMC)

The Central Management Console (CMC) is a web-based tool to perform day-to-day administrative tasks, including user management, content management, and server management. It also allows you to publish, organize, and set security levels for all of your BusinessObjects Enterprise content.

- CMC service

A CMC hosted on a WACS.

- Configuration template

A configuration template stores a list of settings for BusinessObjects Enterprise services. Configuration templates allow you to easily configure multiple instances of servers. There is one configuration template for each service type.

- Connector

WACS provides services through HTTP, HTTP through Proxy, and HTTPS. Each of these is treated as a connector in WACS. There are three connectors.

- Server

In BusinessObjects Enterprise, a server is a running process that can host one or more service.

- Service

A service is an item that provides business functionality from within a server.

- WACS service

A service that provides web application hosting services.

Related Topics

- [Common Tasks](#)

Do I need WACS?

If you plan to use .NET InfoView, and you do not want to use a Java application server to host your CMC, then you can use WACS to host the Central Management Console (CMC).

If you plan to use a supported Java application server to deploy BusinessObjects Enterprise web applications, or if you are installing BusinessObjects Enterprise on a UNIX system, you do not need to install and use WACS.

What are the advantages of using WACS?

Using WACS to host the CMC provides you with a number of advantages:

- WACS requires a minimum effort to install, maintain, and configure.
- All hosted applications are predeployed on WACS, so that no additional manual steps are required.
- WACS is supported by Business Objects.
- WACS removes the need for Java application server administration and maintenance skills.
- WACS provides an administrative interface that is consistent with other Business Objects servers.

Common Tasks

Task	Description	Topic
How can I improve the performance of the Central Management Console (CMC)?	You can improve the performance of the CMC by installing WACS on multiple machines.	<ul style="list-style-type: none"> • Adding or removing additional WACS to your deployment • Cloning a Web Application Container Server
How can I improve the availability of my web-tier?	Create additional WACS in your deployment, so that in the event of a hardware or software failure on one server, another server can continue servicing requests.	Adding or removing additional WACS to your deployment
How can I create an environment where I can easily recover from a misconfigured CMC?	Create a second, stopped, WACS, and use this WACS to define a configuration template. In the event that the primary WACS becomes misconfigured, either use the second WACS until you configure the first server, or apply the configuration template to the first server.	Adding or removing additional WACS to your deployment
How can I improve the security of communication between clients and WACS?	Configure HTTPS on WACS.	<ul style="list-style-type: none"> • Configuring HTTPS/SSL • Using WACS with firewalls

Task	Description	Topic
How can I improve the security of communication between WACS and other Business Objects Enterprise servers in my deployment?	Configure SSL communication between WACS and other Business Objects Enterprise servers in your deployment.	<ul style="list-style-type: none"> • Configuring HTTPS/SSL • Using WACS with firewalls • Configuring servers for SSL
Can I use WACS with HTTPS and a reverse proxy?	You can use WACS with HTTPS and a reverse proxy if you create two WACS and configure both servers with HTTPS. Use the first WACS for communication inside your internal network, and the other WACS for communication with an external network through a reverse proxy.	To configure WACS to support HTTPS with a reverse proxy
How does WACS fit in my IT environment?	WACS can be deployed in an IT environment with existing web servers, hardware load balancers, reverse proxies, and firewalls.	<ul style="list-style-type: none"> • Using WACS with other web servers • Using WACS with a load balancer • Using WACS with a reverse proxy • Using WACS with firewalls
Can I use WACS in a deployment with a load balancer?	You can use WACS in a deployment that uses a hardware load balancer. WACS itself cannot be used as a load balancer.	Using WACS with a load balancer

Task	Description	Topic
Can I use WACS in a deployment with a reverse proxy?	You can use WACS in a deployment that uses a reverse proxy. WACS itself cannot be used as a reverse proxy.	Using WACS with a reverse proxy

Task	Description	Topic
How can I troubleshoot my WACS servers?	If you need to determine the reasons for/causes of the poor performance of your WACS, you can view the log files and view the system metrics.	<ul style="list-style-type: none"> • To view server errors • To view system metrics
I don't get any pages served to me on a particular port. What is wrong?	<p>There are a number of reasons why you might not be able to connect to WACS. Check to see if:</p> <ul style="list-style-type: none"> • The HTTP, HTTP through proxy, and HTTPS ports that you specified for the WACS have been taken by other applications. • The WACS has enough memory allocated to it. • The WACS allows enough concurrent requests. • If necessary, restore the system defaults for the WACS. 	<ul style="list-style-type: none"> • To resolve HTTP port conflicts • To change memory settings • To change the number of concurrent requests • To restore system defaults
Where can I find a list of WACS properties?	The "Server Properties Appendix" of this guide contains a list of WACS properties.	Core Server Settings

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.

Note:

You can deploy more than one WACS on the same machine so that if the primary WACS in your deployment is misconfigured, you can use a secondary WACS to recover your system. However, it is not recommended that you run more than one WACS on a single machine at the same time, due to high resource utilization.

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, CMC availability won't be affected by hardware or software failures on a specific machine, because the other WACS will continue to provide a CMC service.

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

- In a New installation, if you choose to not install a new or configure a pre-existing Java application server, a WACS is automatically installed.

If you select a Java application server in a New installation, WACS is not installed.

- In a Custom or Expand installation, you can choose to install WACS on the "Select Features" screen by expanding **Server Components** 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. A CMC is 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.

WACS is supported only on Windows operating systems.

For more information on installing WACS, see the *SAP BusinessObjects Enterprise XI 3.1 Installation Guide for Windows*.

For information on installing WACS when you're upgrading from BusinessObjects Enterprise XI or XI Release 2, see the *SAP BusinessObjects Enterprise XI Upgrade Guide*.

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. You can view the server state of the WACS through the Central Configuration Manager (CCM).

This delay only occurs 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.

Adding a new Web Application Container Server

Note:

You can deploy more than one WACS on the same machine so that if the primary WACS in your deployment is misconfigured, you can use a secondary WACS to recover your system. However, it is not recommended that you run more than one WACS on a single machine at the same time, due to high resource utilization.

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 **Central Management Console Service**, and click **Next**.
5. On the next "Create New Server" screen, click **Next**.

Note:

Business Objects does not support hosting Web Services SDK and QaaWS (DSWS) or Business Process BI (BPBIWS) web services on WACS. Features or applications using web services, such as Live Office or Federation, are not supported on WACS.

Deploying web services to a WACS in a production deployment is not recommended. However, if you want to test unsupported procedures such as adding or removing web services from WACS and configuring single sign-on for Web Services SDK and QaaWS, see the *Web Application Container Server (WACS): Supported and Unsupported Features for BusinessObjects Enterprise XI 3.1* on the Business Objects customer support site: <http://technicalsupport.businessobjects.com>.

6. On the next "Create Server Screen", select a node to add the server to, type a server name, server port, 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 newly created WACS.

The "Properties" screen appears.

8. In the "Common Settings" pane, ensure that the **Automatically start this server when the Server Intelligence Agent starts** checkbox is unchecked, and click **Save & Close**.

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

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:

You can deploy more than one WACS on the same machine so that if the primary WACS in your deployment is misconfigured, you can use a secondary WACS to recover your system. However, it is not recommended that you run more than one WACS on a single machine at the same time, due to high resource utilization.

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 destination server and services that it hosts have the same settings as the server it was cloned from, with the exception of the server name.

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 Topics

- [To resolve HTTP port conflicts](#)

Deleting WACS servers 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**.

Adding or removing services to WACS

To add a CMC service to a WACS

After you install WACS, a Central Management Console (CMC) service is automatically added to your deployment. There is no need to add a CMC to a WACS unless you create a new WACS without a CMC service, or if you remove a CMC service from a WACS.

To add a CMC service to a WACS, WACS must be installed on the machine. A CMC service can only be added to a WACS that isn't already hosting a CMC.

Adding a CMC service 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 CMC service while you are stopping and adding a web service to the other WACS.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to add the CMC service to, and view the properties of the server to ensure that a CMC service is not already present.
3. Click **Cancel** to return to the "Servers" screen.
4. To stop the WACS that you want to add a CMC service to, right-click the server and click **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 CMC 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 click **Select Services**.
The "Select Services" screen appears.
6. On the "Available services" list, select **Central Management Console Service**, click > to add it to the server, and click **OK**.
7. To start the WACS, right-click the server and click **Start Server**.

The CMC service is added to the Web Application Container Server. The default settings and properties for the CMC are applied.

To remove a CMC service from a WACS

When you remove a CMC service from a WACS, you must ensure that you don't remove the last CMC from your deployment. You need to have at least one additional CMC service running on a WACS in your deployment before you attempt to remove a CMC service.

You cannot delete the last service from a WACS. Therefore, if you are removing a CMC service from a WACS, you must ensure that the server is hosting another 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 CMC from, and view the properties of the server to ensure that a CMC service is present.

3. Click **Cancel** to return to the "Servers" screen.
4. To stop the WACS, right-click the server and click **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 CMC 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 click **Select Services**.
6. On the "Services" list, select **Central Management Console Service**, click **<** to remove it from the server, and click **OK**.
7. To start the WACS, right-click the server and click **Start Server**.

Configuring HTTPS/SSL

You can use the Secure Sockets Layer (SSL) protocol and HTTP for network communication between clients and WACS in your BusinessObjects Enterprise deployment. SSL/HTTPS encrypts network traffic and provides improved security.

There are two types of SSL:

- SSL used between Business Objects servers, including WACS and other BusinessObjects Enterprise servers in your deployment. This is known as CorbaSSL. For more information on using SSL between the Business Objects servers in your deployment, see the "Understanding communication between BusinessObjects Enterprise components" section of the "Working with Firewalls" chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.
- HTTP over SSL, which occurs between WACS and clients (for example, browsers) that communicate with WACS.

Note:

If you are deploying WACS in a deployment with a proxy or reverse proxy, and want to use SSL to secure the network communication in your deployment, you must create two WACS. For more information, see *Using WACS with a reverse proxy*.

To configure HTTPS/SSL on a WACS, you must:

- Generate or obtain a PKCS12 certificate store or JKS keystore which contains your certificates and private keys. You can use Microsoft's

Internet Information Service (IIS) and Microsoft Management Console (MMC) to generate a PKCS12 file, or use openssl or the Java keytool command line tool to generate a keystore file.

- If you want only certain clients to connect to a WACS, then you must generate a certificate trust list file.
- When you have a certificate store and, if necessary, a certificate trust list file, copy the files to the WACS machine.
- Configure HTTPS on the WACS.

Related Topics

- [Understanding communication between BusinessObjects Enterprise components](#)
- [Using WACS with a reverse proxy](#)

To generate a PKCS12 certificate file store

There are many ways of generating a PKCS12 certificate file stores or Java keystores, and tools that you can use. The method that you use depends on the tools that you have access to and are familiar with.

This example demonstrates how to generate a PKCS12 file using Microsoft's Internet Information Services (IIS) and the Microsoft Management Console (MMC).

1. Log on to the machine that hosts WACS as an administrator.
2. In IIS, request a certificate from Certificate Authority. For information on doing this, see the IIS help documentation.
3. Start the MMC by clicking **Start > Run**, typing mmc.exe, and clicking **OK**.
4. Add Certificates Snap-in to the MMC:
 - a. From **File** menu, click **Add/Remove Snap-in**.
 - b. Click **Add**.
 - c. On the "Add Standalone Snap-in" dialog, select **Certificates**, and click **Add**.
 - d. Select **Computer account**, and click **Next**.
 - e. Select **Local Computer**, and click **Finish**.
 - f. Click **Close**, and click **OK**.

The Certificates Snap-In is added to the MMC.

5. In the MMC, expand **Certificates**, and select the certificate that you want to use.
6. On the **Action** menu, select **All Tasks > Export**.
The "Certificate Export Wizard" starts.
7. Click **Next**.
8. Select **Yes, export the private key**, and click **Next**.
9. Select **Personal Information Exchange - PKCS #12 (.PFX)**, and click **Next**.
10. Enter the password you used when you created the certificate and click **Next**. You must specify this password in the **Private Key Access Password** field when you configure HTTPS for the WACS.

A PKCS12 certificate file store is created.

To generate a Certificate Trust List

1. Log on to the machine that hosts WACS as an administrator.
2. Start the Microsoft Management Console (MMC).
3. Add the Internet Information Services Snap-in:
 - a. From the **File** menu, select **Add/Remove Snap-in**, and click **Add**.
 - b. In the "Add Standalone Snap-in" dialog, select **Internet Information Services (IIS) Manager**, and click **Add**.
 - c. Click **Close**, and click **OK**.The IIS snap-in is added to the MMC.
4. In the left pane of the MMC, find the web site for which you want to create the Certificate Trust List.
5. Right-click the web site, and select **Properties**.
6. Click the **Directory Security** tab, and under "Secure Communications", click **Edit**.
7. Click **Enable certificate trust list**, and click **New**.
The "Certificate Trust List Wizard" starts.
8. Click **Next**.
9. Click **Add from Store** or **Add from File**, select the certificate that you want to add to the Certificate Trust List, click **OK**, and click **Next**.
10. Type a name and description for the Certificate Trust List, and click **Next**.

11. Click **Finish**, and then click **OK**.
The Certificate Trust List is displayed in the **Current CTL** field.
12. Select the Certificate Trust List and click **Edit**.
The "Certificate Trust List Wizard" starts.
13. Click **Next**.
14. On the **Current CTL certificates** list, select the Trust List, and click **View Certificates**.
15. Click the **Details** tab, and click **Copy to File**.
The "Certificate Export Wizard" starts.
16. Click **Next**.
17. Select **Yes, export the private key**, and click **Next**.
18. Select **Personal Information Exchange - PKCS #12 (.PFX)**, and click **Next**.
19. Enter the password you used when you created the certificate and click **Next**. You must specify this password in the **Certificate Trust List Private Key Access Password** field when you configure HTTPS for the WACS.

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** checkbox.

HTTPS Configuration

<input type="checkbox"/> Enable HTTPS	
Bind to Hostname or IP Address:	<input type="text" value="localhost"/>
HTTPS Port:	<input type="text" value="443"/>
Proxy Hostname:	<input type="text"/>
Proxy Port:	<input type="text" value="0"/>
Protocol:	<input type="text" value="TLS"/>
Certificate Store Type:	<input type="text" value="PKCS12"/>
Certificate Store File Location:	<input type="text"/>
Private Key Access Password:	<input type="password" value="....."/>
Certificate Alias:	<input type="text"/>
<input type="checkbox"/> Enable Client Authentication	
Certificate Trust List File Location:	<input type="text"/>
Certificate Trust List Private Key Access Password:	<input type="password" value="....."/>

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 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 PKCS12 file or JKS keystore that contains the trust list file.

Note:

The Certificate Trust List type must be the same as the Certificate Store type.

- 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.

Supported authentication methods

WACS supports the following authentication methods:

- Enterprise
- LDAP
- AD Kerberos

WACS does not support the following authentication methods:

- NT
- AD NTLM
- LDAP with Single sign-on
- AD Kerberos Single sign-on

Configuring AD Kerberos for WACS

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.

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

Related Topics

- [Using AD users and groups](#)
- [Windows AD security plug-in](#)
- [Mapping AD accounts](#)
- [Setting up a service account](#)
- [Setting up constrained delegation](#)
- [Configuring the servers](#)
- [Enabling Kerberos authentication in the Windows AD plug-in for WACS](#)
- [Creating configuration files](#)
- [Configuring WACS for AD Kerberos](#)

Enabling Kerberos authentication in the Windows AD plug-in for WACS

In order to support Kerberos, you have to configure the Windows AD security plug-in in the CMC to use Kerberos authentication. This includes:

- Ensuring Windows AD authentication is enabled.
- Entering the AD Administrator account.

Note:

This account requires read access to Active Directory only; it does not require any other rights.

-
- Entering the service principal name (SPN) for the service account.

Prerequisites

Before you configure the Windows AD security plug-in for Kerberos, you must have completed the following tasks:

- [Setting up a service account](#)
- [Granting the service account rights](#)
- [Configuring the servers to use the service account](#)
- [Mapping AD accounts](#)

To configure the Windows AD security plug-in for Kerberos

1. Go to the **Authentication** management area of the CMC.
2. Double-click **Windows AD**.
3. Ensure that the **Windows Active Directory Authentication is enabled** check box is selected.
4. Under **Authentication Options**, select **Use Kerberos authentication**.
5. 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. For example, the Service Account would be *svcacct@DNS.COM* and the SPN would be *BOBJCentralMS/some_name@DOMAIN.COM*.

Note:

- If you plan to allow users from other domains than the default domain to log on, you must provide the SPN you mapped earlier.
- The service account is case sensitive. The case of the account you enter here must match with what is set up in your Active Directory Domain.
- This must be the same account that you use to run the BusinessObjects Enterprise servers or the SPN that maps to this account.

Creating configuration files

The general process of configuring Kerberos on your application server involves these steps:

- Creating the Kerberos configuration file.
- Creating the JAAS login configuration file.

Note:

- The default Active Directory domain must be in uppercase DNS format.

- You don't need to download and install MIT Kerberos for Windows. You also no longer require a keytab for your service account.
- If you are using Vintela Single Sign On the Kerberos and JAAS configuration files are not required.

To create the Kerberos configuration file

Follow these steps to create the Kerberos configuration file.

1. Create the file `krb5.ini`, if it does not exist, and store it under `C:\WINNT` for Windows.

Note:

You can store this file in a different location. However if you do, you need to specify its location in the **Krb5.ini File Location** field on the "Properties" page for the WACS server, in the CMC.

2. Add the following required information in the Kerberos configuration file:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
```

Note:

- `DNS.COM` is the DNS name of your domain which must be entered in uppercase in FQDN format.
- `kdc` is the Host name of the Domain Controller.
- You can add multiple domain entries to the `[realms]` section if your users log in from multiple domains. To see a sample of this file with multiple domain entries, see [Sample Krb5.ini files](#).
- In a multiple domain configuration, under `[libdefaults]` the `default_realm` value may be any of the desired domains. The best practice is to use the domain with the greatest number of users that will be authenticating with their AD accounts.

To create the JAAS login configuration file

1. Create a file called `bscLogin.conf` if it does not exist, and store it in the default location: `C:\WINNT`.

Note:

You can store this file in a different location. However if you do, you will need to specify its location in the **bscLogin.conf File Location** field on the "Properties" page for the WACS server, in the CMC.

2. Add the following code to your JAAS `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {  
com.sun.security.auth.module.Krb5LoginModule required;  
};
```

3. Save and close the file.

Sample Krb5.ini files

Sample multiple domain Krb5.ini file

The following is a sample file with multiple domains:

```
[domain_realm]  
.domain03.com = DOMAIN03.COM  
domain03.com = DOMAIN03.com  
.child1.domain03.com = CHILDL1.DOMAIN03.COM  
child1.domain03.com = CHILDL1.DOMAIN03.com
```

```
.child2.domain03.com = CHILD2.DOMAIN03.COM
child2.domain03.com = CHILD2.DOMAIN03.com
.domain04.com = DOMAIN04.COM
domain04.com = DOMAIN04.com
[libdefaults]
    default_realm = DOMAIN03.COM
    dns_lookup_kdc = true
    dns_lookup_realm = true
[realms]
    DOMAIN03.COM = {
        admin_server = testvmw2k07
        kdc = testvmw2k07
        default_domain = domain03.com
    }
    CHILDD1.DOMAIN03.COM = {
        admin_server = testvmw2k08
        kdc = testvmw2k08
        default_domain = child1.domain03.com
    }
    CHILDD2.DOMAIN03.COM = {
        admin_server = testvmw2k09
        kdc = testvmw2k09
        default_domain = child2.domain03.com
    }
    DOMAIN04.COM = {
        admin_server = testvmw2k011
        kdc = testvmw2k011
        default_domain = domain04.com
    }
}
```

Sample single domain Krb5.ini file

Following is a sample krb5.ini file with a single domain.

```
[libdefaults]
    default_realm = ABCD.MFROOT.ORG
    dns_lookup_kdc = true
    dns_lookup_realm = true
[realms]
    ABCD.MFROOT.ORG = {
        kdc = ABCDIR20.ABCD.MFROOT.ORG
        kdc = ABCDIR21.ABCD.MFROOT.ORG
        kdc = ABCDIR22.ABCD.MFROOT.ORG
        kdc = ABCDIR23.ABCD.MFROOT.ORG
        default_domain = ABCD.MFROOT.ORG
    }
}
```

Configuring WACS for AD Kerberos

After you've configured the machine that is hosting WACS for AD Kerberos authentication, you must configure the WACS itself, through the Central Management Console (CMC).

To configure WACS for AD Kerberos



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.

Troubleshooting Kerberos

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Kerberos configuration

To enable Kerberos logging

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 .

Note:

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

The "Web Tier Configuration" screen appears.

5. Under **Command Line Parameters**, copy the following text to the end of the parameters:

```
"-Dcrystal.enterprise.trace.configuration=verbose  
-Djcsi.kerberos.debug=true"
```

6. Click **OK**.
7. On the "Manage Servers" screen, start the WACS.

To test your Kerberos configuration

- Run the following command to test your Kerberos configuration, where `servact` is the service account and domain under which the CMS is running, and `password` is the password associated with the service account.

```
<Install Directory>\Business Objects\javas  
dk\bin\kinit.exe servact@TESTM03.COM Password
```

For example:

```
C:\Program Files\Business Objects\javas  
dk\bin\kinit.exe servact@TESTM03.COM Password
```

If you still have a problem, ensure that the case you entered for your domain and service principal name match exactly with what is set in Active Directory.

Mapped AD user unable to log on to BusinessObjects Enterprise on WACS

The following two issues may occur, despite the fact that the users have been mapped to BusinessObjects Enterprise:

- *Logon failure due to different AD UPN and SAM names*
- *Pre-authentication error*

Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to BusinessObjects Enterprise. Despite this fact, they are unable to successfully log on to CMC with AD authentication and Kerberos in the following format:

DOMAIN\ABC123

This problem can happen when the user is set up in Active Directory with a UPN and SAM name that are not the same, either in case or otherwise.

Following are two examples which may cause a problem:

- The UPN is abc123@company.com but the SAM name is DOMAIN\ABC123.
- The UPN is jsmith@company but the SAM name is DOMAIN\johnsmith.

There are two ways to address this problem:

- Have users log in using the UPN name rather than the SAM name.
- Ensure the SAM account name and the UPN name are the same.

Pre-authentication error

A user who has previously been able to log on, can no longer log on successfully. The user will receive this error: Account Information Not Recognized. The WACS logs reveal the following error: "Pre-authentication information was invalid (24) "

This can occur because the Kerberos user database didn't get a change made to UPN in AD. This may mean that the Kerberos user database and the AD information are out of sync.

To resolve this problem, reset the user's password in AD. This will ensure the changes are propagated correctly.

WACS and your IT environment

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

Using WACS with other web servers

When a Web Application Container Server (WACS) is installed, it works as an application server and a web server without requiring any extra

configuration. You can configure supported web servers like Internet Information Services (IIS) and Apache to perform URL forwarding to the WACS server.

Note:

Request forwarding from IIS by using an ISAPI filter to WACS is not supported.

WACS does not support a deployment scenario where a web server hosts static content and WACS hosts dynamic content. Static and dynamic content must always reside on WACS.

Using WACS with a load balancer

To use WACS in a deployment with a hardware load balancer, you must configure the load balancer so that it uses either IP routing or active cookies. This way, once a user's session is established on one WACS, all subsequent requests by the same user are sent to the same WACS.

WACS is not supported with hardware load balancers using passive cookies.

If your hardware load balancer forwards SSL-encrypted HTTPS requests to your WACS, then you must configure HTTPS on the WACS, and install SSL certificates on every WACS.

If your hardware load balancer decrypts HTTPS traffic and forwards decrypted HTTP requests to your WACS, then no additional WACS configuration is required.

Related Topics

- [Configuring HTTPS/SSL](#)

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.

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.

Configuration of HTTP through Proxy

<input type="checkbox"/>	Enable HTTP through Proxy
<input checked="" type="checkbox"/>	Bind to All IP Addresses
Bind to Hostname or IP Address:	<input type="text" value="localhost"/>
HTTP Port:	<input type="text" value="6406"/>
Proxy Hostname:	<input type="text"/>
Proxy Port:	<input type="text" value="0"/>

4. Click **Save & Close**.

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.

Using WACS with firewalls

Deploying WACS in an IT environment with firewalls is supported.

By default, WACS bind to all IP addresses on the machine that it is installed on. If you plan to use a firewall between clients and your WACS, you must force WACS to bind to a specific IP address for HTTP or HTTP through proxy. To do this, uncheck **Bind to All IP Addresses**, and then specify a Hostname or IP address to bind to.

If you plan to use a firewall between a WACS server and the other Business Objects servers in your deployment, see the “Working with Firewalls” chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

Configuring 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 "HTTPS 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 Business Objects servers in your deployment.
6. Click **Save & Close**.
7. Restart the WACS.

Troubleshooting

To view server errors

The log file is located in the `<InstallDir>/Logging` directory, where `<InstallDir>` is the directory where BusinessObjects Enterprise is installed.

The name of the log file is in the format `<servername>_<datestarted>_<timestarted>_<processId>.log`, where `<servername>` is the name of the WACS, `<datestarted>` is the date that the WACS was started, `<timestarted>` is the time it was started, and `<processId>` is the server's process ID.

Note:

All errors are written to the log file. No error messages are written to the Windows Event Viewer.

To change the logging level

You can change the logging severity through the CMC. The levels of severity are:

Logging Level	Description
DEBUG	Logs all WACS activity. This option logs the most amount of information. It is not recommended to select DEBUG in a production environment.
INFO	Logs general information. Selecting INFO also logs WARN , ERROR , and FATAL messages to the log file.
WARN	Logs a message when the application encounters a problem. Selecting WARN also logs ERROR and FATAL messages to the log file.

Logging Level	Description
ERROR	Logs a message when a service encounters an error or is not available. Selecting ERROR also logs FATAL messages to the log file.
FATAL	Logs a message when an event occurs that results in the failure of the server or service that it provides.
AUTO	Retrieves the logging level that is specified in the WACS command line. By default, this value is ERROR .

To change the logging level of a WACS:

1. Go to the "Servers" management area of the CMC.
2. Double-click the server.
Stopping the server is not required.
The "Properties" screen appears.
3. On the **Log Level** list, select a logging severity level, and click **OK**.
4. On the "Servers" screen, restart the WACS.

To view system metrics

You can view the system 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**.

A list of system metrics appears. For a descriptions of the metrics that are on the list, see *WACS metrics*.

Related Topics

- [WACS metrics](#)

WACS metrics

The following table describes the metrics that appear on the "Metrics" screen.

Metric	Description
"Total Memory (MB)"	The total memory used by WACS, in mega bytes.
"List Running WACS Connectors"	A list of all running connectors.
WACS Connector(s) Failed at Start-up	Whether there are any failed connectors. If true, at least one connector failed. If false, all connectors are running.

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 new server state called "Started with Errors". A WACS that is in this state is running, but has at least one misconfigured HTTP, HTTP through Proxy, or HTTPS connector.

If a WACS status is "Started with Errors", go to the "Metrics" page and view the "Running WACS Connector" metric. If an enabled connector does not appear in the list, the connector has not been configured properly.

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 Running WACS Connectors and WACS Startup Errors metrics. If the HTTP, HTTP through Proxy, or HTTP connectors do not appear in the Running WACS Connectors list, 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.

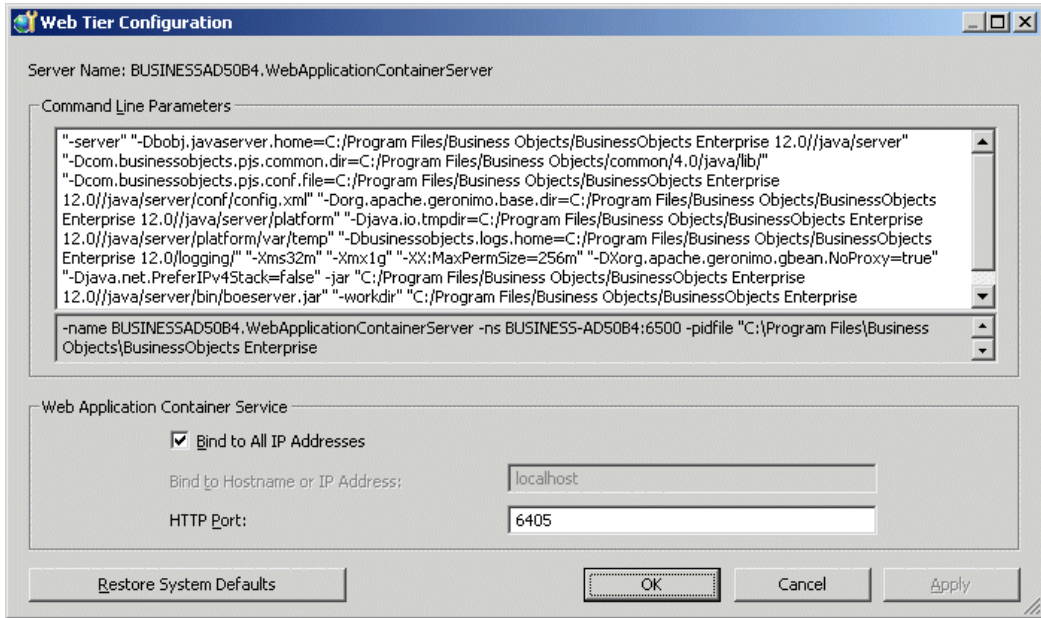
To resolve HTTP port conflicts

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 .

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.

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**.

To change memory settings

To improve the server performance of a WACS, you can change the amount of memory that is allocated to the server through the Central Configuration Manager (CCM).

1. Start the CCM, and click the **Manage Servers** icon .
2. Specify the logon credentials for the CMC.
3. On the "Manage Servers" screen, stop the WACS.
4. Click the **Web Tier Configuration** icon .

Note:

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

The "Web Tier Configuration" screen appears.

5. Under "Command Line Parameters", specify a new memory value by editing the command line:
 - a. Find the -Xmx option. This option normally has a value specified.
For example "-Xmx1g". This setting allocates one giga byte of memory to the server.
 - b. Specify a new value for the parameter.
 - To specify a value in mega bytes, use "m". For example, "-Xmx640m" allocates 640 mega bytes of memory to the WACS.
 - To specify a value in giga bytes, use "g". For example, "-Xmx2g" allocates two giga bytes of memory to the WACS.
 - c. Click **OK**.
6. On the "Manage Servers" screen, start the WACS.



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. 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**.

To restore system defaults

If you've misconfigured a WACS, you can restore the system defaults through the Central Configuration Manager (CCM).

1. Start the 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 .

Note:

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

The "Web Tier Configuration" screen appears.

5. Click **Restore System Defaults**.
6. If necessary, specify a free HTTP port, and click **OK**.

7. On the "Manage Servers" screen, start the WACS.

To prevent users from connecting to WACS through HTTP

In certain cases, you may want to only allow 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 only accepts 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. Uncheck **Bind to all IP Addresses**.
4. In the **Bind to Hostname or IP address** field, type 127.0.0.1, and click **OK**.
5. To start the WACS, right-click the server and click **Start Server**.
The WACS that is configured this way only accepts connections from the local machine.

WACS properties

For a complete list of the general, HTTP, HTTP through Proxy, and HTTPS configuration properties that can be configured for WACS, see the "Core Server Settings" section of the "Server Properties Appendix".

Related Topics

- [Core Server Settings](#)



Modifying Default Security Behavior



10 chapter

BusinessObjects Enterprise and reverse proxy servers

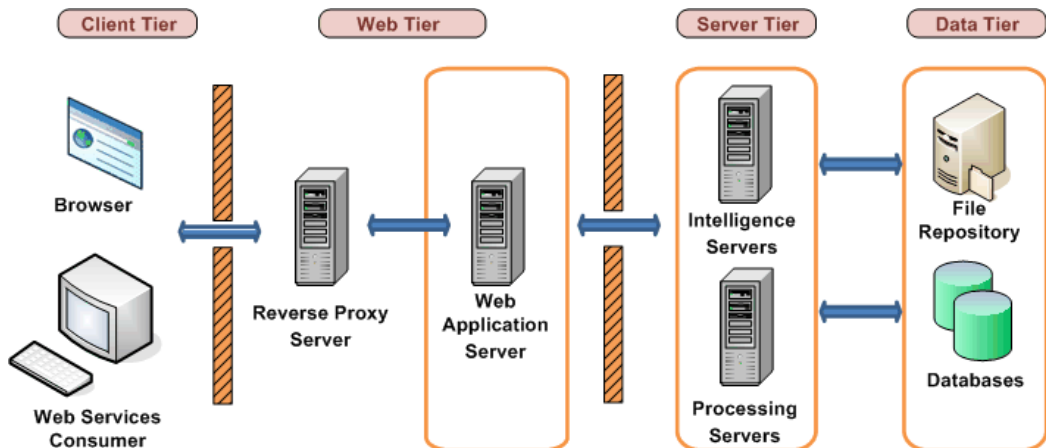
This section explains how to configure BusinessObjects Enterprise and reverse proxy servers to work together.

Introduction to reverse proxy servers

BusinessObjects Enterprise can be deployed in an environment with one or more reverse proxy servers. A reverse proxy server is typically deployed in front of the web application servers in order to hide them behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, hiding private IP addresses.

Because the reverse proxy server translates the public URLs to internal URLs, it must be configured with the URLs of the BusinessObjects Enterprise web applications that are deployed on the internal network.

The following diagram shows a typical deployment with a reverse proxy server. LiveOffice is a typical web services consumer application. InfoView and CMC are typical applications used from a browser.



Supported reverse proxy servers

BusinessObjects Enterprise supports reverse proxy servers that can adjust the value of the `path` attribute in Set-Cookie headers. For example:

- IBM Tivoli Access Manager WebSEAL 6 (WebSEAL 6)
- Apache 2.2

In addition BusinessObjects Enterprise supports the Microsoft ISA 2006 as a reverse proxy server.

Understanding how BusinessObjects Enterprise web applications are deployed

BusinessObjects Enterprise web applications are deployed on a web application server. If the web application server is located behind a reverse proxy server, the reverse proxy server should be configured with the context paths of the BusinessObjects Enterprise WAR files. To expose all of the BusinessObjects Enterprise functionality, configure a context path for every BusinessObjects Enterprise WAR file that is installed.

Note:

If some WAR files are installed but their context paths are not configured in the reverse proxy server, some parts of CMC and InfoView may not be functional.

The following table gives an example of typical WAR files that are used by common BusinessObjects Enterprise web applications. For a complete list of WAR files, refer to the Installation and Configuration guide.

In the following table, “X” indicates a WAR file that is required for an application to function. “xx” indicates a WAR file that is used by an application. If the WAR file indicated by “xx” is not available, some functionality in the application will not be available. For example, if the path to `CrystalReports.war` is not configured in the reverse proxy server, Crystal Reports functionality will not be available in CMC and InfoView.

	CMC	In foView	Crystal Reports	Desktop Intelli- gence	Web In- telli- gence
AnalyticalReporting.war	xx	xx		X	X
CmcApp.war	X				
CmcAppActions.war	X				
CrystalReports.war	xx	xx	X		
InfoViewApp.war		X			
InfoViewAppActions.war		X			
OpenDocument.war			X	X	X
PlatformServices.war	X	X	X	X	X

Configuring reverse proxy servers for BusinessObjects Enterprise web applications

The reverse proxy server must be configured to map incoming URL requests to the correct web application in deployments where BusinessObjects Enterprise web applications are deployed behind a reverse proxy server.

This section contains specific configuration examples for some of the supported reverse proxy servers. Refer to the vendor documentation for your reverse proxy server for more information.

To configure the reverse proxy server

1. Ensure the reverse proxy server is set up correctly according to the vendor's instructions and the deployment's network topology.
2. Determine which BusinessObjects Enterprise web applications are deployed and which WAR files are required.
3. Configure the reverse proxy server for each BusinessObjects Enterprise web application. Note that the rules are specified differently on each type of reverse proxy server.
4. Perform any special configuration that is required. Some Business Objects web applications require special configuration when deployed on certain web application servers.

Related Topics

- [Detailed instructions for configuring reverse proxy servers for BusinessObjects Enterprise](#)
- [To configure Apache 2.2 reverse proxy server for BusinessObjects Enterprise](#)
- [To configure WebSEAL 6.0 reverse proxy server for BusinessObjects Enterprise](#)
- [Special configuration for BusinessObjects Enterprise in reverse proxy deployments](#)

Detailed instructions for configuring reverse proxy servers for BusinessObjects Enterprise

This section contains information to help you successfully set up your reverse proxy server.

Ensure all required WAR files have been configured

BusinessObjects Enterprise web applications are deployed in WAR files on a web application server. Different BusinessObjects Enterprise web

applications require different WAR files. Ensure you configure a directive on your reverse proxy server for every WAR file that is required for your deployment.

Declare longer context path strings first

On the reverse proxy server, the directives for `InfoViewAppActions` must exist before the directives for `InfoViewApp`. The directives for `CmcAppActions` must exist before the directives for `CmcApp`.

Deploy the applications and actions in the same parent folder

The web applications `CmcApp` and `CmcAppActions` must be deployed under the same parent folder. The web applications `InfoViewApp` and `InfoViewAppActions` must be deployed under the same parent folder.

InfoView and CMC applications can be renamed

You can rename the `InfoView.war` file and the `CMC.war` file in the `ProxyPass` and `ProxyPassReverseCookiePath` directives. You cannot change the name of any other BusinessObjects Enterprise WAR files.

Use the '/' character consistently

Define the context paths in the reverse proxy server in the same way as they are entered in a browser URL. For example, if the directive contains a '/' at the end of the mirror path on the reverse proxy server, enter '/' at the end of the browser URL.

Ensure the '/' character is used consistently in the source and destination URL in the directive of the reverse proxy server. If the '/' character is added at the end of the source URL, it must also be added to the end of the destination URL.

Related Topics

- [Understanding how BusinessObjects Enterprise web applications are deployed](#)

To configure Apache 2.2 reverse proxy server for BusinessObjects Enterprise

This section explains how to configure BusinessObjects Enterprise and Apache 2.2 to work together.

1. Ensure that BusinessObjects Enterprise and Apache 2.2 are installed on separate machines.
2. Ensure that Apache 2.2 is installed and configured as a reverse proxy server as described in the vendor documentation.
3. Configure the `ProxyPass` for every web application that is deployed behind the reverse proxy server.
4. Configure the `ProxyPassReverseCookiePath` for every web application that is deployed behind the reverse proxy server.

Example:

This example uses `boe-deploy-server.domain.com` for the web application server domain and `XIR3` for the mirror path. Replace these values with the appropriate values for your deployment.

```
ProxyPass /XIR3/CmcAppActions http://boe-deploy-server.domain.com:port/CmcAppActions
ProxyPassReverseCookiePath /CmcAppActions /XIR3/CmcAppActions
ProxyPass /XIR3/CmcApp http://boe-deploy-server.domain.com:port/CmcApp
ProxyPassReverseCookiePath /CmcApp /XIR3/CmcApp
ProxyPass /XIR3/InfoViewAppActions http://boe-deploy-server.domain.com:port/InfoViewAppActions
ProxyPassReverseCookiePath /InfoViewAppActions /XIR3/InfoViewAppActions
ProxyPass /XIR3/InfoViewApp http://boe-deploy-server.domain.com:port/InfoViewApp
ProxyPassReverseCookiePath /InfoViewApp /XIR3/InfoViewApp
ProxyPass /XIR3/PlatformServices http://boe-deploy-server.domain.com:port/PlatformServices
ProxyPassReverseCookiePath /PlatformServices /XIR3/PlatformServices
ProxyPass /XIR3/AnalyticalReporting http://boe-deploy-server.domain.com:port/AnalyticalReporting
```

```
ProxyPassReverseCookiePath /AnalyticalReporting
/XIR3/AnalyticalReporting
ProxyPass /XIR3/CrystalReports http://boe-deploy-server.domain.com:port/CrystalReports
ProxyPassReverseCookiePath /CrystalReports /XIR3/CrystalReports
ProxyPass /XIR3/OpenDocument http://boe-deploy-server.domain.com:port/OpenDocument
ProxyPassReverseCookiePath /OpenDocument /XIR3/OpenDocument
ProxyPass /XIR3/PerformanceManagement http://boe-deploy-server.domain.com:port/PerformanceManagement
ProxyPassReverseCookiePath /PerformanceManagement
/XIR3/PerformanceManagement
```

To configure WebSEAL 6.0 reverse proxy server for BusinessObjects Enterprise

This section explains how to configure BusinessObjects Enterprise and WebSeal 6.0 to work together.

The recommended configuration method is to create a single standard junction that maps all of the BusinessObjects web applications hosted on an internal web application server or web server to a single mount point.

1. Ensure that BusinessObjects Enterprise and WebSEAL 6.0 are installed on separate machines.

It is possible but not recommended to deploy BusinessObjects Enterprise and WebSEAL 6.0 on the same machine. Refer to the WebSEAL 6.0 vendor documentation for instructions on configuring this deployment scenario.

2. Ensure that WebSeal 6.0 is installed and configured as described in the vendor documentation.
3. Launch the WebSeal **pdadmin** command line utility. Log in to a secure domain such as **sec_master** as a user with administration authorization.
4. Enter the following command at the **padmin sec_master** prompt:

```
server task <instance_name-webseald-host_name> create -t
<type> -h <host_name> -p <port> <junction_point>
```

Where:

- `<instance_name-webseald-host_name>` specifies the full server name of the installed WebSEAL instance. Use this full server name in the same format as displayed in the output of the `server list` command.
- `<type>` specifies the type of junction. Use `tcp` if the junction maps to an internal HTTP port. Use `ssl` if the junction maps to an internal HTTPS port.
- `<host_name>` specifies the DNS host name or IP address of the internal server that will receive the requests.
- `<port>` specifies the TCP port of the internal server that will receive the requests.
- `<junction_point>` specifies the directory in the WebSEAL protected object space where the document space of the internal server is mounted.

Example:

```
server task default-webseald-webseal.rp.businessob
jects.com create -t tcp -h 10.50.130.123 -p 8080 /hr
```

To configure Microsoft ISA 2006 for BusinessObjects Enterprise

This section explains how to configure BusinessObjects Enterprise and ISA 2006 to work together.

The recommended configuration method is to create a single standard junction that maps all of the BusinessObjects web applications hosted on an internal web application server or web server to a single mount point. Depending on your web application server, there are additional configuration required on the application server for it to work with ISA 2006.

1. Ensure that BusinessObjects Enterprise and ISA 2006 are installed on separate machines.

It is possible but not recommended to deploy BusinessObjects Enterprise and ISA 2006 on the same machine. Refer to the ISA 2006 documentation for instructions on configuring this deployment scenario.

2. Ensure that ISA 2006 is installed and configured as described in the vendor documentation.
3. Launch the ISA Server Management utility.
4. Use the navigation panel to launch a new publishing rule

a. Go to

Arrays > MachineName > Firewall Policy > New > Web Site Publishing Rule

Remember:

Replace `MachineName` with the name of the machine on which ISA 2006 is installed.

- b. Type a rule name in **Web publishing rule name** and click **Next**
- c. Select **Allow** as the rule action and click **Next**.
- d. Select **Publish a single Web site or load balancer** as the publishing type and click **Next**.
- e. Select a connection type between the ISA Server and the published Web site and click **Next**.
 For example, select **Use non-secured connections to connect the published Web server or server farm**.
- f. Type the internal name of the Web site you are publishing (e.g machine name hosting BusinessObjects Enterprise) in **Internal site name** and click **Next**.

Note:

If the machine hosting ISA 2006 cannot connect to the target server select **Use a computer name or IP address to connect to the published server** and type the name or IP address in the field provided.

- g. In "Public Name Details" select the domain name (e.g. **Any domain name**) and specify any internal publishing details (e.g. /*). Click **Next**.
 You now need to create a new web listener to monitor for incoming Web requests.

5. Click **New** to launch the New Web Listener Definition Wizard.
 - a. Type a name in **Web Listener name** and click **Next**.
 - b. Select a connection type between the ISA Server and the published Web site and click **Next**.
 For example, select **Do not require SSL secured connections with clients**.
 - c. In "Web Listener IP Addresses" select the following and click **Next**.

- Internal
- External
- Local Host
- All Networks

ISA Server is now configured to only publish over HTTP.

- d. Select an "Authentication Setting" option and click **Next** and then **Finish**.

The new listener is now configured for the web publishing rule.

6. Click **Next** in "User Sets" then **Finish**.
7. Click **Apply** to save all the settings for the web publishing rule and update the ISA 2006 configuration

You now have to update the properties of the web publishing rule to map paths for the BusinessObjects web applications.

8. In the navigation panel, right-click the Firewall Policy you configured and select **Properties**.
9. Select the "Paths" tab and click **Add** to map routes to BusinessObjects web applications.

Use the mapping in the table below for the CMC and Java InfoView

From	To
/AnalyticalReporting/*	/Product/AnalyticalReporting/*
/CmcApp/*	/Product/CmcApp/*
/CmcAppActions/*	/Product/CmcAppActions/*
/CrystalReports/*	/Product/CrystalReports/*
/InfoViewApp/*	/Product/InfoViewApp/*
/InfoViewAppActions/*	/Product/InfoViewAppActions/*
/OpenDocument/*	/Product/OpenDocument/*
/PerformanceManagement/*	/Product/PerformanceManagement/*

From	To
/PlatformServices/*	/Product/PlatformServices/*
/BusinessProcessBI/*	Product/BusinessProcessBI/*
/dswsbobje/*	/Product/dswsbobje/*

Use the mapping in the table below for .NET InfoView

From	To
/Analyticalreporting/*	/Product/Analyticalreporting/*
/CrystalReports/*	/Product/CrystalReports/*
/crystalreportviewers12/*	/Product/crystalreportviewers12/*
/InfoViewApp/*	/Product/InfoViewApp/*
/InfoViewAppActions/*	/Product/InfoViewAppActions/*
/OpenDocument/*	/Product/OpenDocument/*
/PlatformServices/*	/Product/PlatformServices/*

10. Under "Public Name" tab, select **Request for the following websites** and click **Add**.
11. In the "Public Name" dialog type your ISA 2006 server name and click **OK**.
12. Click **Apply** to save all the settings for the web publishing rule and update the ISA 2006 configuration
13. Verify the connections by accessing the following URL:

`http://<ISA Server host Name>:<web listener port number>/<External path of the application>`

For Example: `http://myISAServer:80/Product/InfoViewApp`

Note:

You may have to refresh the browser several times.

You need to modify the HTTP policy for the rule have just configured to ensure that you will be able to logon on to the CMC. Right-click the rule you created in the ISA Server Management utility and select **Configure HTTP**. You must now deselect **Verify Normalization** in the "URL Protection" area.

To remotely access BusinessObjects Enterprise you need to create an access rule.

Related Topics

- [Enabling the root path for session cookies for ISA 2006](#)
- [Using WACS with a reverse proxy](#)

Special configuration for BusinessObjects Enterprise in reverse proxy deployments

Some BusinessObjects Enterprise products need additional configuration to function correctly in reverse proxy deployments. This section explains how to perform the additional configuration.

Enabling reverse proxy for Developer Suite Web Services

This section describes the required procedures to enable reverse proxies for Developer Suite Web Services.

To enable reverse proxy on Tomcat

To enable reverse proxy on the Tomcat web application server, you must modify the `server.xml` file. Required modifications include setting `proxyPort` as the reverse proxy server listen port and adding a new `proxyName`. This section explains the procedure.

1. Stop Tomcat.
2. Open the `server.xml` for Tomcat.

On Windows, `server.xml` is located at `<CATALINA_HOME>\conf`. The default value of `<CATALINA_HOME>` is `C:\Program Files\Business Objects\Tomcat55`.

On UNIX `server.xml` is located at `<CATALINA_HOME>/conf`. The default value of `<CATALINA_HOME>` is `<INSTALLDIR>/bobje/tomcat55`

3. Locate this section in the `server.xml` file:

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!--See proxy documentation for more information about
using
    this.-->
<!--
    <Connector port="8082"
        maxThreads="150" minSpareThreads="25" maxS
pareThreads="75"
        enableLookups="false"
        acceptCount="100" debug="0" connectionTime
out="20000"
        proxyPort="80" disableUploadTimeout="true" />
-->
```

4. Uncomment the Connector element by removing `<!--` and `-->`.
5. Modify the value of `proxyPort` to be the reverse proxy server listen port.
6. Add a new `proxyName` attribute to the Connector's attribute list. The value of the `proxyName` must be the proxy server name which should be resolvable to the correct IP address by Tomcat.

Example:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082
-->
    <!--See proxy documentation for more information
about using
        this.-->
        <Connector port="8082"
            maxThreads="150" minSpareThreads="25" maxS
pareThreads="75"
            enableLookups="false"
            acceptCount="100" debug="0" connectionTime
out="20000"
            proxyName="my_reverse_proxy_server.domain.com"

            proxyPort="ReverseProxyServerPort"
            disableUploadTimeout="true" />
```

Where `my_reverse_proxy_server.domain.com` and `ReverseProxyServerPort` should be substituted by the correct reverse proxy server name and its listen port.

7. Save and close the `server.xml` file.

8. Restart Tomcat.
9. Ensure the reverse proxy server maps its virtual path to the correct Tomcat connector port. In the above example, the port is 8082.

The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy Business Objects Web Services deployed on Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
ProxyPassReverseCookiePath /dswsbobje
/XI3.0/dswsbobje
```

To enable Webservices, the proxy name and port number have to be identified for the connector.

Enabling reverse proxy for Developer Suite Web Services on web application servers other than Tomcat

The following procedure requires that BusinessObjects Enterprise web applications are successfully configured against your chosen web application server. Note that the `wsresources` are case-sensitive.

1. Stop the web application server.
2. Specify the external URL of the Web Services in the `dsws.properties` file.

This file is located in `dswsbobje` web application. For example if your external URL is `http://my_reverse_proxy_server.do/main.com/XI3.0/dswsbobje/`, update the following properties in the `dsws.properties` file:

- `wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.do/main.com/XI3.0/dswsbobje/services/ReportEngine`
- `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.do/main.com/XI3.0/dswsbobje/services/BICatatalog`
- `wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.do/main.com/XI3.0/dswsbobje/services/Publish`

- `wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.do main.com/XI3.0/dswsbobje/services/QueryService`
- `wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.do main.com/XI3.0/dswsbobje/services/BIPlatform`
- `wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.do main.com/XI3.0/dswsbobje/services/LiveOffice`

3. Save and close the `dsws.properties` file.
4. Restart the web application server.
5. Ensure the reverse proxy server maps its virtual path to the correct web application server connector port. The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy Business Objects Web Services deployed on the web application server of your choice:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:<listening port> /dswsbobje
```

```
ProxyPassReverseCookiePath /dswsbobje /XI3.0/dswsbobje
```

Where `<listening port>` is the listening port of your web application server.

Enabling the root path for session cookies for ISA 2006

This section describes how to configure specific web application servers to enable the root path for session cookies to work with ISA 2006 as the reverse proxy server.

To configure Tomcat 5.5

To configure the root path for session cookies to work with ISA 2006 as the reverse proxy server, add the following to the `<Connector>` element in `server.xml`:

```
emptySessionPath="true"
```

1. Stop Tomcat
2. Open the `server.xml` which is located in:
`<CATALINA_HOME>\conf`
3. Locate the following section in the `server.xml` file:

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!-- See proxy documentation for more information about
using this -->
<!--
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxS
pareThreads="75" enableLookups="false"
acceptCount="100" debug="0" connectionTimeout="20000"

proxyPort="80" disableUploadTimeout="true" />
-->
```

4. Uncomment the Connector element by removing `<!--` and `-->`.
5. To configure the root path for session cookies to work with ISA 2006 as the reverse proxy server, add the following to the `<Connector>` element in `server.xml`:

```
emptySessionPath="true"
```

6. Modify the value of `proxyPort` to be the reverse proxy server listen port.
7. Add a new `proxyName` attribute to the Connector's attribute list. The value must be the proxy server name which should be resolvable to the correct IP address by Tomcat.

For example:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!-- See proxy documentation for more information about
using
this -->
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxS
pareThreads="75"
enableLookups="false" emptySessionPath="true"
acceptCount="100" debug="0" connectionTimeout="20000"

proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

8. Save and close the `server.xml` file.
9. Restart Tomcat.

Ensure the reverse proxy server maps its virtual path to the correct Tomcat connector port. In the above example, the port is 8082.

To configure Sun Java 8.2

You need to modify the `sun-web.xml` for every BusinessObjects Enterprise web application.

1. Go to `<SUN_WEBAPP_DOMAIN>\generated\xml\j2ee-modules\<WAR_FILE>\WEB-INF\`
2. Open `sun-web.xml`
3. After the `<context-root>` container add the following:

```
<session-config>
  <cookie-properties>
    <property name="cookiePath" value="/" />
  </cookie-properties>
</session-config>
<property name="reuseSessionID" value="true"/>
```

4. Save and close `sun-web.xml`.
5. Repeat steps 1-4 for every web application.

To configure Oracle Application Server 10gR3

You need to modify the `global-web-application.xml` or `orion-web.xml` for every BusinessObjects Enterprise web application's deployment directory.

1. Go to `<ORACLE_HOME>\j2ee\home\config\`
2. Open `global-web-application.xml` or `orion-web.xml`.
3. Add the following line to the `<orion-web-app>` container:

```
<session-tracking cookie-path="/" />
```

4. Save and close the configuration file.
5. Logon to the Oracle Admin Console:
 - a. Go to **OC4J:home > Administration > Server Properties**.
 - b. Select **Options** under "Command Line Options".
 - c. Click **Add another Row** and type the following:

```
Doracle.useSessionIDFromCookie=true
```

6. Restart the Oracle server.

To configure WebSphere Community Edition 2.0

1. Open the WebSphere Community Edition 2.0 Admin Console.
2. In the left navigation panel find "Server" and select **Web Server**.
3. Select the connectors and click **Edit**.
4. Select the **emptySessionPath** checkbox and click **Save**.
5. Type your ISA server name in **ProxyName**.
6. Type the ISA listener port number in **ProxyPort**.
7. Stop and then restart the connector.

Enabling reverse proxy for BusinessObjects Live Office

To enable BusinessObjects Live Office's View Object in Web Browser feature for reverse proxies, adjust the default viewer URL. This can be done in the Central Management Console (CMC) or through Live Office options.

Note:

This section assumes reverse proxies for Business Objects Java InfoView and Business Objects Web Services have been successfully enabled.

Related Topics

- [Enabling reverse proxy for Developer Suite Web Services](#)

To adjust the default viewer URL using the CMC

1. Log on to the CMC.
2. Navigate to the Applications page and click **CMC**.
3. Select **Processing Extensions** from the **Actions** menu.
4. In the URL field, set the correct default viewer URL and click **Set URL**.
For example:

```
http://ReverseProxyServer:ReverseProxyServerPort/ProxiedInfoView/opendoc/openDocument.jsp?sIDType=CUID&iDocID=%SI_CUID%
```

Where `ReverseProxyServer` and `ReverseProxyServerPort` are the correct reverse proxy server name and its listen port. `ProxiedInfoView` is the correct virtual path for Java InfoView.

To adjust the default view URL using Live Office options

1. On the LiveOffice menu click **Options** and then click the **Enterprise** tab.
2. Select **Specify the URL** to view the report in repository and type the correct URL in the adjacent field. For example:

```
http://ReverseProxyServer:ReverseProxyServerPort/ProxiedInfoView/opendoc/openDocument.jsp
```


Where `ReverseProxyServer` and `ReverseProxyServerPort` are the correct reverse proxy server name and its listen port. `ProxiedInfoView` is the correct virtual path for Java InfoView.

Enabling reverse proxy for Business Process BI Web Services

To enable reverse proxies for Business Process BI Web Services, you must adjust the default viewer URL and enable reverse proxy on the web application server.

Related Topics

- [To adjust the default viewer URL using the CMC](#)
- [Enabling reverse proxy for Developer Suite Web Services](#)

Enabling reverse proxy for Business Process BI on web application servers other than Tomcat

Note:

The following procedure requires that BusinessObjects Enterprise web applications are successfully configured for your chosen web application server. Note that the `wsresources` are case-sensitive.

1. Stop the web application server.
2. Ensure the reverse proxy server maps its virtual path to the correct web application server connector port. The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy BusinessObjects web services deployed on the web application server of your choice:

```
ProxyPass /BusinessProcessBI http://internalServer:<listening
port>/BusinessProcessBI
ProxyPassReverseCookiePath /BusinessProcessBI
http://internalServer:<listening port>/BusinessProcessBI
```

10 | Modifying Default Security Behavior

Special configuration for BusinessObjects Enterprise in reverse proxy deployments

Where `<listening port>` is the listening port of your web application server.



Improving Performance

11

chapter



Improving performance

It is good practice to regularly assess the performance of your system and make changes to account for future growth and potential problem areas.

First, you need to assess the current performance of your system. You can assess your system's performance by talking to your users and delegated administrators, and by studying your system metrics. When you have an idea of potential problem areas, you can compare your system's performance to expected service thresholds.

After you identify performance issues, you can take steps to account for them by scaling your system or adjusting your configuration settings.

- [Assessing your system's performance](#)
- [Performance risks and solutions](#)

Note:

This section is for improving the performance of an existing deployment. For information about if you haven't deployed your system yet, see the BusinessObjects Enterprise Deployment Planning guide.

Assessing your system's performance

Before you change your settings to enhance performance, you need to determine how well your system is currently performing. BusinessObjects Enterprise provides server metrics that allow you to monitor and assess your current processing problem areas.

To effectively assess your system's performance, you need to:

- Assess user needs.

Get qualitative feedback from your users. See [Assessing user needs](#).

- Analyze server metrics.

Check the server and system logs. For detailed instructions, see [Analyzing server metrics](#).

- Evaluate the performance of each server component.

Compare the current system usage to recommended service thresholds. Determine the required number of processors, services, and machines. For more information, see [Evaluating your system's performance](#).

Assessing user needs

Talk to your users and delegated administrators. They can help you determine which areas of your system are currently experiencing performance issues, if any. They can also let you know where to anticipate higher system traffic in the future. And there may be areas of the system that are not being used at all.

For example, if your organization is hiring new people in the finance department, the usage of financial reports will probably increase. If the financial reports are Web Intelligence documents, you may need to add a Web Intelligence Processing Server to handle the extra processing load. Or if you're planning to switch from Web Intelligence documents to Crystal reports, you may not need a Web Intelligence Processing Server at all.

It is good practice to conduct a company-wide survey concerning BusinessObjects Enterprise usage in order to capture all of the current problems and future changes. Ask your users about current performance concerns, their average daily usage, and their anticipated future usage:

- What types of tasks are they performing and how often?
- Have they noticed slow performance when performing particular tasks?
- What types of objects do they use most often?
- Have they noticed slow performance when using particular types of objects?
- Do they anticipate increasing or decreasing their use of the system in the near future?
- Are they hiring new people?
- Do they plan to use BusinessObjects Enterprise to perform more tasks in the future?

In particular, talk to publishers and determine what their Publishing needs are. Some publishers require additional capacity for high-volume publications that deliver personalized instances to many destinations and recipients. For

example, a publisher at an insurance company may run a billing publication that generates thousands of personalized report instances for customers. This scenario requires a deployment that can handle the high processing load.

It is good practice to regularly re-assess your organization's needs. Follow the steps you used when planning your deployment. For detailed instructions, see the BusinessObjects Enterprise Deployment Planning Guide.

When you have a sense of the organization's performance issues, you can verify them by viewing the current system metrics.

Analyzing server metrics

After you assess user needs, you can verify your users' current performance concerns by monitoring system activity. Server metrics may also reveal other areas where high server traffic may be an issue.

The CMC allows you to view server metrics over the Web. These metrics include general information about each machine, along with details that are specific to the type of server. The CMC also allows you to view system metrics, which include information about your product version, your CMS, and your current system activity.

Tip:

For an example of how to use server metrics in your own web applications, see the "View Server Summary" sample on the BusinessObjects Enterprise Admin Launchpad.

Click the appropriate link to jump to that section:

- [Viewing current server metrics](#)
- [Viewing system metrics](#)

Viewing current server metrics

The Servers management area of the CMC displays server metrics that provide statistics and information about each BusinessObjects Enterprise server. The general information displayed for each server includes information about the machine that the server is running on—its name, operating system, total hard disk space, free hard disk space, total RAM, number of CPUs, and

local time. The general information also includes the time the server started and the version number of the server.

To view server metrics

1. Go to the **Servers** management area of the CMC.
2. Click the server whose metrics you want to view.
3. Choose **Properties** from the **Manage** menu.
4. In the Properties dialog box, click **Metrics** in the navigation list.

The Metrics tab displays additional, server-specific information for some servers. The Metrics tab is only for viewing information about the servers. For information about changing server settings, see [To change a server's properties](#).

Additional server metrics

Input and Output File Repository Servers

For each File Repository Server, the Metrics tab provides the following metrics for:

- data sent and data written
- the number of active files and active client connections
- the total available hard disk space

For information about changing these settings, see [Setting root directories and idle times of the File Repository Servers](#).

Central Management Server

For the CMS, the Metrics tab provides the following additional metrics:

- the number of jobs that are failed, pending, running, completed, or waiting
- the number of licenses
- CMS system database information

For information about configuring the Central Management Server, see [Configuring server settings](#).

Connection Server

For the Connection Server, the Metrics tab lists additional information about the types of datasources the Connection Server currently uses. Listed network layers and associated databases have been set as active datasources in the global configuration file of the Connection Server.

For more information about configuring the Connection Server, see the *Data Access Guide*.

Job Servers

The Metrics tabs of these servers lists the following metrics:

- the location of its temporary files
- the processing mode
- the current number of jobs that are being processed
- the total number of requests received
- the total number of failed job creations
- the types of default destinations currently enabled

For information about changing these settings, see [Configuring the processing tier for enhanced performance](#).

Note:

This applies to all types of Job Servers, including Crystal Reports Job Servers, Program Job Servers, Destination Job Servers, List of Values Job Servers, Desktop Intelligence Job Servers, and Web Intelligence Job Servers.

Crystal Reports Cache Server

For each Cache Server, the Metrics tab provides the following metrics:

- the number of bytes transferred
- the number of current connections
- the current cache size
- the number of requests served
- the cache hit rate
- the number of requests that are queued

The Metrics tab also displays the current values for the following settings, which can be changed on the Properties tab:

- the number of minutes before an idle job is closed
- whether or not the database is accessed whenever a viewer's file (object) is refreshed
- the location of the cache files
- the maximum cache size
- the number of minutes between refreshes from the database

The Metrics tab also provides a table that lists the Processing Servers that the Cache Server has connections to, along with the number of connections made to each Processing Server.

For information about changing these settings, see [Modifying Cache Server performance settings](#).

Desktop Intelligence Cache Server

For each Desktop Intelligence Cache Server, the Metrics tab provides the following metrics:

- the current cache size
- the number of bytes transferred
- the number of current connections
- the number of requests served
- the cache hit rate
- the number of requests that are queued

The Metrics tab also displays the current values for the following settings, which can be changed on the Properties tab:

- the maximum cache size
- the location of the cache files
- the number of minutes before an idle job is closed
- the number of minutes between refreshes from the database

- whether or not the database is accessed whenever a viewer's file (object) is refreshed
- the number of documents to keep in the cache when the cache is full
- whether or not to share report data between clients

The Metrics tab also provides a table that lists the processing servers that the Desktop Intelligence Cache Server has connections to, along with the number of connections made to each server.

For information about changing these settings, see [Modifying Cache Server performance settings](#).

Note:

This server processes information only for Desktop Intelligence documents.

Event Server

For the Event Server, the Metrics tab displays statistics for each file that the server is monitoring, including the file name and the last time the event occurred.

For information about changing these settings, see [Modifying the polling time of the Event Server](#).

Desktop Intelligence Processing Server

For the Desktop Intelligence Processing Server, the Metrics tab provides the following metrics:

- the number of current connections
- the current number of open processing threads running
- the total number of requests served
- the total bytes transferred
- the number of requests queued
- the maximum number of child processes
- the number of failed requests

The Metrics tab also displays the current values for the following settings, which can be changed on the Properties tab:

- the location of temporary files
- idle connection timeout
- the maximum number of simultaneous report jobs
- the maximum number of operations allowed before resetting a report job
- whether a viewer refresh always hits the database
- whether or not report jobs are shared
- the number of minutes before an idle report job is closed
- the number of preloaded report jobs
- whether or not to share report data between clients
- the oldest processed data given to a client

For information about these settings, see [Desktop Intelligence Server Settings](#).

Note:

This server processes information only for Desktop Intelligence documents.

Crystal Reports Processing Server

For the Crystal Reports Processing Server, the Metrics tab provides the following metrics:

- the number of current connections
- the number of requests queued
- the number of requests served
- the number of failed requests
- the total bytes transferred

The Metrics tab also displays the current values for the following settings, which can be changed on the Properties tab:

- the number of minutes before an idle connection is closed
- the location of temporary files
- the maximum number of simultaneous report jobs

- the minutes before a report job is closed
- the oldest processed data given to a client
- whether a viewer refresh always hits the database
- the maximum number of child processes

For information about changing these settings, see [Crystal Reports Server Settings](#).

Note:

This server processes information only for Crystal Reports objects.

Web Intelligence Processing Server

For the Web Intelligence Processing Server, the Metrics tab provides the number of current requests and the total number of requests.

The Metrics tab also displays the current values for the following settings, which can be changed on the Properties tab:

- the maximum number of connections
- the number of minutes before an idle connection is closed
- whether or not to enable document caching
- whether or not to enable real-time caching
- the number of minutes allowed for document caching
- the size of the document cache
- whether or not to enable list of values caching
- the batch size for lists of values
- the maximum size allowable for custom sorting a list of values
- the size of the universe cache
- the percentage of documents to keep in the cache when the cache is full
- the maximum number of minutes allowed for scanning the document cache
- the maximum number of downloaded documents to cache
- the maximum size of binary and character files

For information about these settings, see [Web Intelligence Server Settings](#).

Note:

This server processes information only for Web Intelligence documents.

Report Application Server

The Metrics tab of the Report Application Server (RAS) shows the number of reports that are open, and the number of reports that have been opened. It also shows the number of open connections, along with the number of open connections that have been created.

For information about these settings, see [Crystal Reports Server Settings](#).

Viewing system metrics

The Settings management area of the CMC displays system metrics that provide general information about your BusinessObjects Enterprise installation. The "Properties" section includes information about the product version and build. It also lists the data source, database name, and database user name of the CMS database. The "View global system metrics" section lists current account activity, along with statistics about current and processed jobs. The "Cluster" section lists the name of the CMS you are connected to, the name of the CMS cluster, and the names of other cluster members.

To view system metrics

1. Go to the **Settings** management area of the CMC.
2. Click the arrows to expand and view the settings for the **Properties**, **View global system metrics**, and **Cluster** sections.
 - For information about licenses and account activity, see [Managing Licenses](#).
 - For information about CMS clusters, see [Clustering Central Management Servers](#).

Logging server activity

BusinessObjects Enterprise allows you to log specific information about BusinessObjects Enterprise web activity. For details on locating and customizing the web activity logs, see [Auditing web activity](#).

- In addition, each of the BusinessObjects Enterprise servers is designed to log messages to your operating system's standard system log.
 - On Windows NT/2000, BusinessObjects Enterprise logs to the Event Log service. You can view the results with the Event Viewer (in the Application Log).
 - On UNIX, BusinessObjects Enterprise logs to the syslog daemon as a User application. Each server prepends its name and PID to any messages that it logs.

Each server also logs assert messages to the logging directory of your product installation. The programmatic information logged to these files is typically useful only to Business Objects support staff for advanced debugging purposes. The location of these log files depends upon your operating system:

- On Windows, the default logging directory is `C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\Logging`
- On UNIX, the default logging directory `INSTALL_ROOT/bobje/logging` directory of your installation.

The important point to note is that these log files are cleaned up automatically, so there will never be more than approximately 1 MB of logged data per server.

Note:

To enable logging to function on UNIX machines that are hosting BusinessObjects Enterprise servers, you must set up and configure system logging so that all messages logged to the “user” facility of “info” level or higher are recorded. Setup procedures vary from system to system. Consult your operating system documentation for specific instructions.

Evaluating your system's performance

After you collect enough anecdotal and statistical information about your BusinessObjects Enterprise deployment, you can begin to isolate problem areas.

Use the server metrics to verify the user feedback. Do the server metrics confirm your users' performance concerns? If not, the performance issue may be caused by something besides your BusinessObjects Enterprise configuration, such as your network speed, the structure of the database, or the complexity of your report design.

Then compare the current usage to the recommended service thresholds. By comparing these numbers, you can rate each server's performance and create a list of minor, moderate, and major performance risks.

To evaluate your system's performance

1. Make a list of all server components in your deployment.
2. For each server component, compare the information you received from your users to the server metrics in the Central Management Console.

Note:

For information, see [Analyzing server metrics](#).

3. Compare the server's current traffic metrics to the recommended service thresholds. Pay particular attention to the number of simultaneous requests and user connections.

For information about thresholds and estimates, see the BusinessObjects Enterprise Deployment Planning Guide.

4. Sort the server components into the following categories:

Minor performance risk	A server component is considered a minor risk if a low percentage of your users report performance problems and the server metrics do not reflect the same problems.
------------------------	--

Moderate performance risk	A server component is considered a moderate risk if the server metrics show that the current usage is close to the limit of the recommended service thresholds. You may also want to flag a server component as a moderate risk if a high percentage of users report performance issues, or if you expect an increase in usage that will cause the current usage numbers to meet the service thresholds.
Major performance risk	A server component is considered a major performance risk if the server metrics show that current usage significantly exceeds the minimum service thresholds. You may also want to flag a server component as a major risk if you expect a substantial increase in usage that will cause the usage numbers to exceed the service thresholds.

5. After you isolate the key problem areas and the severity of the performance issues, proceed to the next section: [Performance risks and solutions](#).

Resolving performance issues

After you assess your system and determine the potential trouble areas, you can develop a strategy for resolving performance issues. The appropriate solution for each server depends on the level of performance risk and the type of server.

Note:

For more information about evaluating your system's performance, see [Evaluating your system's performance](#).

- For minor or moderate performance issues, users encounter occasional performance issues or your system approaches the limits of the recommended service thresholds. You may be able to resolve these issues by fine-tuning your system configuration.

For more information, see [Configuring the intelligence tier for enhanced performance](#) and [Configuring the processing tier for enhanced performance](#).

- For major performance issues, your server traffic significantly exceeds the recommended service thresholds. You should consider expanding the system by adding servers to account for the problem areas.

For more information about scaling considerations, see [Scaling your system](#). For installation instructions, see the BusinessObjects Enterprise Installation Guide.

For example, when you install a default deployment of Business Objects Enterprise, one Web Intelligence Processing Server is installed by default. This deployment will easily meet your needs if you have under 20 concurrent active users accessing the Web Intelligence Processing Server by working with xCelsius or Web Intelligence documents. If you have 20 to 30 users accessing the Web Intelligence Processing Server, you may encounter some performance issues because you are reaching the limits of the recommended service threshold. To account for some of these problems, you can tweak the Web Intelligence Processing Server settings. (For details, see [Web Intelligence Server Settings](#).) However, if your traffic is significantly higher than the service threshold (such as 50 concurrent active users using the Web Intelligence Report Server) then you need to scale your system to include more instances of the Web Intelligence Processing Server service.

The following table provides a quick reference for troubleshooting performance for each type of server component:

Performance risks and solutions

Server type	Performance risk	Solutions
CMS	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> Because the CMS manages the entire system, problems that appear to be CMS issues may be caused by the server components managed by the CMS. It is good practice to check the performance of all other services before adding new CMS services. For other information about advanced CMS configuration, see Server management overview.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> Install additional CMS services. For information, see Increasing overall system capacity.
Event Server	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> Change how often the Event Server checks for file events. For more information, see Modifying the polling time of the Event Server.

Server type	Performance risk	Solutions
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> It is unlikely that you will encounter major performance issues with the Event Server. However, it is good practice to install one Event Server for each CMS. For information about installing additional Event Servers, see Scaling your system.
Cache Server	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> You can resolve many issues by changing Cache Server properties such as the maximum cache size and the number of minutes between database refreshes. For more information, see Modifying Cache Server performance settings.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> If your system exceeds 400 simultaneous requests, install an additional Cache Server. See Scaling your system.

Server type	Performance risk	Solutions
Job Servers	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> If the number of simultaneous jobs does not exceed the recommended threshold of 20 jobs, check the Maximum Jobs Allowed setting. For more information, see Core Server Settings.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> If the Job Server is running more than 20 simultaneous jobs on average, install another Job Server service. See Scaling your system.
Desktop Intelligence Processing Server	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> If the number of concurrent active users does not exceed 25, try changing the settings. See Desktop Intelligence Server Settings.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> If the number of concurrent active users exceeds 25, install addition servers. See Scaling your system.

Server type	Performance risk	Solutions
Web Intelligence Processing Server	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> If the number of concurrent active users does not exceed 25, try changing the settings. See Web Intelligence Server Settings.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> If the number of concurrent active users exceeds 25, install additional servers. See Increasing scheduled reporting capacity.
Report Application Server	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> To adjust the Report Application Server's settings for connection idle time and the maximum number of simultaneous threads, see Crystal Reports Server Settings.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> If your users run more than 200 simultaneous requests, install additional Report Application Servers. For more information, see Increasing on-demand viewing capacity for Crystal reports.

Server type	Performance risk	Solutions
Crystal Reports Processing Server	<ul style="list-style-type: none"> Minor/moderate 	<ul style="list-style-type: none"> You can change how a Crystal Reports Processing Server handles data and user connections by fine-tuning its settings. See Crystal Reports Server Settings.
	<ul style="list-style-type: none"> Major 	<ul style="list-style-type: none"> If the Crystal Reports Processing Server is handling more than 400 simultaneous viewing sessions, install more processing servers. For more information, see Increasing on-demand viewing capacity for Crystal reports.

Configuring the intelligence tier for enhanced performance

This section provides instructions for configuring settings for components from the intelligence tier. You can adjust the settings to account for minor and moderate performance issues.

Note:

For more information about the intelligence tier, see [Configuring server settings](#).

Configuring the intelligence tier includes:

- [Configuring the CMS](#)

- [Modifying the polling time of the Event Server](#)
- [Configuring the File Repository Servers](#)
- [Modifying Cache Server performance settings](#)

Configuring the CMS

Because the CMS manages the entire system, problems that appear to be CMS issues are often caused by the server components managed by the CMS. It is good practice to check the performance of all other services before changing the CMS settings or adding and clustering new CMS services.

Settings for the CMS are already discussed in great detail in the “Managing and Configuring Servers” chapter. A list of CMS properties can be found in the “Core Server Settings” section of the “Server Properties Appendix”.

Related Topics

- [Configuring server settings](#)
- [Core Server Settings](#)
- [Clustering Central Management Servers](#)

Modifying the polling time of the Event Server

The Properties tab of the Event Server allows you to change the frequency with which the Event Server checks for file events. This "Event Poll Interval" setting determines the number of seconds that the server waits between polls. The minimum value is 1 (one). It is important to note that, the lower the value, the more resources the server requires.

To modify the polling time

1. Go to the **Servers** management area of the CMC.
2. Select the Event Server whose settings you want to change.
3. Choose **Properties** from the **Manage** menu.
4. On the **Properties** tab, provide a new value for the Event Poll Interval field.

Note:

The value that you type must be 1 or greater.

5. Click **Save** or **Save & Close**.

Configuring the File Repository Servers

The Properties tabs of the Input and Output File Repository Servers allow you to set the maximum idle time. For more information, see [Setting root directories and idle times of the File Repository Servers](#). For a full list of Input and Output File Repository Server settings, see [Core Server Settings](#).

Modifying Cache Server performance settings

The Properties tab of the Cache Server allows you to set the location of the cache files, the maximum cache size, the maximum number of simultaneous processing threads, the number of minutes before an idle job is closed, and the number of minutes between refreshes from the database.

To modify Cache Server performance settings

1. Go to the **Servers** management area of the CMC.
2. Select the Cache Server whose settings you want to change.
3. Choose **Properties** from the **Manage** menu.
4. Make your changes on the **Properties** tab.
5. Click **Save** or **Save & Close**.

Configuring the processing tier for enhanced performance

This section provides instructions for configuring settings for components from the processing tier.

Note:

For more information about the processing tier, see [Configuring server settings](#).

Configuring the processing tier includes modifying the performance settings for the following server types:

- Job Servers.

For a list of Job Server properties, see “Core Server Settings”.

By default, job servers run jobs as independent processes rather than as threads. This method allows for more efficient processing of large, complex reports.

- Desktop Intelligence Report Servers and Desktop Intelligence Processing Servers.
- Web Intelligence Report Servers and Web Intelligence Processing Servers.
- Report Application Servers and Crystal Reports Processing Servers.

Note:

The RAS must have been installed and configured in order to use the List of Values Job Server.

Related Topics

- [Core Server Settings](#)
- [Desktop Intelligence Server Settings](#)
- [Web Intelligence Server Settings](#)
- [Crystal Reports Server Settings](#)

To change a server's properties

1. Go to the "Servers" management area of the CMC.
2. Select the server whose settings you want to change.
3. Choose **Properties** from the **Manage** menu.
4. Make the changes you want, then click **Save** or **Save & Close**.

Note:

Not all changes occur immediately. If a setting cannot change immediately, the Properties dialog box display both the current setting (in red text) and the desired setting. When you return to the Servers management area, the server will be marked as Stale. When you restart the server, it will use the desired settings from the Properties dialog box and the Stale flag is removed from the server.

Scaling your system

The BusinessObjects Enterprise architecture allows for a multitude of server configurations, ranging from stand-alone, single-machine environments, to large-scale deployments supporting global organizations.

For information about adding and deleting servers from your BusinessObjects Enterprise installation, see [Adding, cloning, and deleting servers](#)

This section provides information about system scalability and the BusinessObjects Enterprise servers that are responsible for particular aspects of your system. Each subsection focuses on one aspect of your system's capacity, discusses the relevant components, and provides a number of ways in which you might modify your configuration accordingly.

Before modifying these aspects of your system, it is strongly recommended that you contact your Business Objects sales representative and request information about the *SAP BusinessObjects Enterprise Sizing Guide*. A Business Objects Services consultant can then assess your reporting environment and assist in determining the configuration that will best integrate with your current environment.

General scalability considerations include the following:

- *Increasing overall system capacity*
- *Increasing scheduled reporting capacity*
- *Increasing on-demand viewing capacity for Crystal reports*
- *Increasing prompting capacity*
- *Enhancing custom web applications*
- *Improving web response speeds*
- *Getting the most from existing resources*

Increasing overall system capacity

As the number of report objects and users on your system increases, you can increase the overall system capacity by clustering two (or more) Central Management Servers (CMS). You can install multiple CMS services/daemons on the same machine. However, to provide server redundancy and fault-tolerance, you should ideally install each cluster member on its own machine.

CMS clusters can improve overall system performance because every BusinessObjects Enterprise request results, at some point, in a server component querying the CMS for information that is stored in the CMS database. When you cluster two CMS machines, you instruct the new CMS to share in the task of maintaining and querying the CMS database.

For more information, see [Clustering Central Management Servers](#).

Increasing scheduled reporting capacity

Increasing Crystal reports processing capacity

All Crystal reports that are scheduled are eventually processed by a Job Server. You can expand BusinessObjects Enterprise by running individual Report Job Servers on multiple machines, or by running multiple Report Job Servers on a single multi-processor machine.

If the majority of your reports are scheduled to run on a regular basis, there are several strategies you can adopt to maximize your system's processing capacity:

- Install the Job Server in close proximity to (but not on the same machine as) the database server against which the reports run. Ensure also that the File Repository Servers are readily accessible to all Job Server (so they can read report objects from the Input FRS and write report instances to the Output FRS quickly). Depending upon your network configuration, these strategies may improve the processing speed of the Job Server, because there is less distance for data to travel over your corporate network.
- Verify the efficiency of your reports. When designing reports in Crystal Reports, there are a number of ways in which you can improve the performance of the report itself, by modifying record selection formulas, using the database server's resources to group data, incorporating parameter fields, and so on. For more information, see the "Designing Optimized Web Reports" section in the *Crystal Reports User's Guide* (version 8.5 and later).
- Use event-based scheduling to create dependencies between large or complex reports. For instance, if you run several very complex reports on a regular, nightly basis, you can use Schedule events to ensure that the reports are processed sequentially. This is a useful way of minimizing the processing load that your database server is subject to at any given point in time.
- If some reports are much larger or more complex than others, consider distributing the processing load through the use of server groups. For instance, you might create two server groups, each containing one or more Job Servers. Then, when you schedule recurrent reports, you can specify that it be processed by a particular server group to ensure that especially large reports are distributed evenly across resources.

- Increase the hardware resources that are available to a Job Server. If the Job Server is currently running on a machine along with other BusinessObjects Enterprise components, consider moving the Job Server to a dedicated machine. If the new machine has multiple CPUs, you can install multiple Job Servers on the same machine (typically no more than one service/daemon per CPU).

Increasing Web Intelligence document processing capacity

All Web Intelligence documents that are scheduled are eventually processed by a Web Intelligence Job Server and Web Intelligence Processing Server. You can expand BusinessObjects Enterprise by running individual Web Intelligence Processing Servers on multiple machines, or by running multiple Web Intelligence Processing Servers on a single multi-processor machine.

When running multiple Web Intelligence Processing Servers, you don't need to duplicate the Web Intelligence Job Server. One Web Intelligence Job Server can be used to drive multiple Web Intelligence Processing Servers. However, if you are working with server groups, a Web Intelligence Job Server must exist in the same group as the Web Intelligence Processing Servers.

Note:

When deciding whether to increase the number Web Intelligence Processing Servers, keep in mind that Web Intelligence Processing Server processes both scheduling and viewing requests, whereas requests for Crystal reports are processed by three separate servers, the Report Job Server, the Crystal Reports Cache Server and Crystal Reports Processing Server.

Increasing on-demand viewing capacity for Crystal reports

When you provide many users with View On Demand access to reports, you allow each user to view live report data by refreshing reports against your database server. For most requests, the Crystal Reports Processing Server retrieves the data and performs the report processing, and the Crystal Reports Cache Server stores recently viewed report pages for possible reuse. However, if users use the Advanced DHTML viewer, the Report Application Server (RAS) processes the request.

If your reporting requirements demand that users have continual access to the latest data, you can increase capacity in the following ways:

- Increase the maximum allowed size of the cache. For details, see [Modifying Cache Server performance settings](#).
- Verify the efficiency of your reports. When designing reports in Crystal Reports, there are a number of ways in which you can improve the performance of the report itself, by modifying record selection formulas, using the database server's resources to group data, incorporating parameter fields, and so on. For more information, see the "Designing Optimized Web Reports" section in the *Crystal Reports User's Guide* (version 8.5 and later).
- Increase the number of Crystal Reports Processing Servers that service requests on behalf of Cache Servers. You can do this by installing additional Processing Servers on multiple machines. However, do not install more than one Processing Server per machine; the Processing Server automatically creates new server instances based on demand.
- Increase the number of Crystal Reports Processing Servers, Cache Servers, and Report Application Servers on the system, and then distribute the processing load through the use of server groups. For instance, you might create two server groups, each containing one or more Cache Server/Processing Server pairs along with one or more Report Application Servers. You can then specify individual reports that should always be processed by a particular server group.

Increasing prompting capacity

When reports use a list of values, the RAS processes on-demand list-of-values objects for the report when the report is being viewed. Scheduled list-of-values objects are processed by the List of Values Job Server without using RAS.

To avoid contention with other applications that use the RAS, you can add a RAS server that will be dedicated to processing list-of-value objects. In CMC you can then create a RAS server group and assign the dedicated RAS to the RAS server group. In Business View Manager, you then assign the list-of-values objects to be processed by the RAS server group.

Enhancing custom web applications

If you are developing your own custom desktops or administrative tools with the BusinessObjects Enterprise Software Development Kit (SDK), be sure to review the libraries and APIs. You can now, for instance, incorporate complete security and scheduling options into your own web applications.

You can also modify server settings from within your own code in order to further integrate BusinessObjects Enterprise with your existing intranet tools and overall reporting environment.

To improve the scalability of your system, consider distributing administrative efforts by developing web applications for delegated content administration. You can grant select users the ability to manage particular BusinessObjects Enterprise folders, content, users, and groups on behalf of their team, department, or regional office.

In addition, be sure to check the developer documentation available on your BusinessObjects Enterprise product CD for performance tips and other scalability considerations. The query optimization section in particular provides some preliminary steps to ensuring that custom applications make efficient use of the query language.

Improving web response speeds

Because all user interaction with BusinessObjects Enterprise occurs over the Web, you may need to investigate a number of areas to determine exactly where you can improve web response speeds. These are some common aspects of your deployment that you should consider before deciding how to expand BusinessObjects Enterprise:

- Assess your web server's ability to serve the number of users who connect regularly to BusinessObjects Enterprise. Use the administrative tools provided with your web server software (or with your operating system) to determine how well your web server performs. If the web server is indeed limiting web response speeds, consider increasing the web server's hardware.
- If web response speeds are slowed only by report viewing activities, see [Increasing scheduled reporting capacity](#) and [Increasing on-demand viewing capacity for Crystal reports](#).
- Take into account the number of users who regularly access your system. If you are running a large deployment, ensure that you have set up a CMS cluster. For details, see [Increasing overall system capacity](#).

If you find that a single application server inadequately services the number of scripting requests made by users who access your system on a regular basis, increase the hardware resources that are available to the application server. If the application server is currently running on the web server, or on

a single machine with other BusinessObjects Enterprise components, consider moving the application server to a dedicated machine.

Note:

BusinessObjects Enterprise does not support the session-replication functionality provided by some Java web application servers.

Getting the most from existing resources

One of the most effective ways to improve the performance and scalability of your system is to ensure that you get the most from the resources that you allocate to BusinessObjects Enterprise.

Click the appropriate link to jump to that section:

- [Optimizing network speed and database efficiency](#)
- [Using the appropriate processing server](#)
- [Optimizing BusinessObjects Enterprise for report viewing](#)

Optimizing network speed and database efficiency

When thinking about the overall performance and scalability of BusinessObjects Enterprise, don't forget that BusinessObjects Enterprise depends upon your existing IT infrastructure. BusinessObjects Enterprise uses your network for communication between servers and for communication between BusinessObjects Enterprise and client machines on your network. Make sure that your network has the bandwidth and speed necessary to provide BusinessObjects Enterprise users with acceptable levels of performance. Consult your network administrator for more information.

BusinessObjects Enterprise processes reports against your database servers. If your databases are not optimized for the reports you need to run, then the performance of BusinessObjects Enterprise may suffer. Consult your database administrator for more information.

Using the appropriate processing server

When users view a report using the Advanced DHTML viewer, the report is processed by the Report Application Server rather than the Crystal Reports Processing Server and Cache Server. The Report Application Server is optimized for report modification. For simple report viewing you can achieve better system performance if users select the DHTML viewer, the Active X

viewer, or the Java viewer. These report viewers process reports against the Crystal Reports Processing Server.

If the ability to modify reports is not needed at your site, you can disable the Advanced DHTML viewer for all users of BusinessObjects Enterprise.

Disabling the Advanced DHTML Viewer

1. In the Central Management Console, go to the **Applications** management area.
2. Select **Web Desktop**, then choose **Properties** from the **Manage** menu.
3. In the **Viewers** area, clear the option labeled **Allow users to use the Advanced DHTML Viewer**.
4. Click **Update**.

Optimizing BusinessObjects Enterprise for report viewing

BusinessObjects Enterprise allows you to enable data sharing, which permits different users accessing the same report object to use the same data when viewing a report on demand or when refreshing a report. Enabling data sharing reduces the number of database calls, thereby reducing the time needed to provide report pages to subsequent users of the same report while greatly improving overall system performance under load. However, to get full value from data sharing, you must permit data to be reused for some period of time. This means that some users may see "old" data when they view a report on demand, or refresh a report instance that they are viewing.

For details on data sharing options for reports, see the *SAP BusinessObjects Enterprise Administrator's Guide*. For more information on configuring BusinessObjects Enterprise to optimize report viewing in your system, see the planning section in the *SAP BusinessObjects Enterprise Installation Guide*.

Improving Publishing performance

As an administrator, you may be required to perform deployment configuration and troubleshooting tasks on behalf of publishers to optimize Publishing performance. This section contains general deployment recommendations and specific server configuration tips. For troubleshooting information related to publication design, see the "Recommendations and Troubleshooting for Publications" chapter in the *SAP BusinessObjects Enterprise Publisher's Guide*.

General deployment recommendations

Recommendations for disk usage

Follow these disk usage recommendations to improve Publishing performance:

- Ensure your server machines and peripheral devices have the speed and capability to handle high-volume publications.
- Use multiple striped disks.
- Move the Output File Repository Server (FRS) to a dedicated clustered node with striped disks.
- Physically separate the Input FRS and Output FRS.
- Provide the Input FRS and Output FRS with separate disk controllers.

Recommendations for server machines

Follow these recommendations for your server machines:

- In Windows, to reduce the time required to create files, use the fsutil behavior set `disable8dot3` command to disable the creation of 8.3 short file names. You must restart your computer for this setting to take effect. For more information, see the article available at <http://support.microsoft.com/kb/121007>.
- Ensure that the CPU, RAM, and hard disk on the CMS database machine is powerful enough for high-volume scenarios.

Configuring servers in the CMC to optimize Publishing performance

In general, you can do the following to optimize server performance for Publishing:

- In the "Servers" area of the CMC, disable unnecessary servers. For example, if you are running a Crystal reports publication only, you can disable Desktop Intelligence and Web Intelligence servers. However, before you do this, ensure that the servers that you want to disable are not being used by other users in the system.

- For Job Servers that are used in Publishing, ensure that **Maximum Concurrent Jobs** is set to five per CPU. To do this, in the "Servers" area, select the Job Server and click **Manage > Properties**.

Consider changing the level of detail logged by the Adaptive Processing Server.

Note:

Increasing the level of detail in log files may affect server performance.

The default (and recommended) setting for the level of detail in log files is **ERROR**. However, you or your publisher may want to increase the level of detail in Adaptive Processing Server log files to better track the progress of publication jobs. To do this, in the "Servers" area, select the Adaptive Processing Server and click **Manage > Properties**. On the "Log level" list, select **INFO**. **INFO** gives you more details such as the following:

- The publication has been delivered successfully to a recipient.
- A batch of recipients has been processed successfully.
- Post-processing publication extensions have been initialized.

Configure the Adaptive Processing Server to handle more jobs.

The following recommendations can improve the performance of the Adaptive Processing Server:

- If several publications are running concurrently, create multiple instances of the Adaptive Processing Server. In general, it is recommended that you have one Adaptive Processing Server instance for every three concurrent publications.
- Increase the heap size for the Adaptive Processing Server. To do this, click **Manage > Properties**, and add the following to the command-line parameter: `-Xmx1024M`.
- Run the Publishing Service and Publishing Post-Processing Service on different instances of the Adaptive Processing Server.

If your publisher wants to enable auditing and clean-up, configure auditing for the CMS so that it logs all details.

For high-volume publications, it is recommended that the publisher enable clean-up to delete unnecessary files generated by the publication job and conserve server space. To do this, during the publication design process, the publisher will deselect the default Enterprise location as a destination.

If auditing has been enabled for Publishing, you must configure the CMS to support this scenario so that the details of the deleted files are still recorded. In the "Servers" area, select the CMS and click **Manage > Properties**. In the dialog box that appears, click **Audit Events** on the navigation list. Ensure **Auditing is Enabled** and **Object Deleted** are selected.

Ensure that the email settings are configured properly for the Destination Job Server.

Publications that are intended for email destinations may fail because email has not been configured properly as a destination for the Destination Job Server. In the "Servers" area of the CMC, double-click the Destination Job Server. In the "Properties" dialog box, click **Destination** on the navigation list to ensure the following:

- **Email** has been added as a destination.
- The values in the **Domain Name**, **Host**, and **Port** fields are correct.
- The **To** field contains %SI_EMAIL_ADDRESS%.

Increase the number of concurrent jobs that the Destination Job Server can process.

If publications are intended for the default Enterprise location or an unmanaged disk destination, and you use striped disks for the Output FRS, it is recommended that you set the maximum number of concurrent jobs as the number of disks multiplied by five.

If the publisher uses Crystal report dynamic recipient sources, ensure the Report Application Server (RAS) is configured correctly.

The RAS must be configured to read at least the same number of database records as the number of recipients in the dynamic recipient source. For instance, to process a dynamic recipient source with data for 100,000 recipients, the RAS must be set to read more than 100,000 database records.

To check this setting, in the "Servers" area of the CMC, select the RAS and go to **Manage > Properties**. In the **Number of database records to read when previewing or refreshing a report** field, ensure the number is correct or enter a new number.

Resolving “Out of memory” errors

If the publisher receives the error message

`java.lang.OutOfMemoryError: unable to create new native thread` when a high-volume publication is run, it is because the Adaptive Processing Server and Publishing Service have insufficient stack memory to handle the number of Publishing threads that are generated. This error can occur if stack memory is designated as Java heap space.

You can set a thread limit for the Adaptive Processing Server. In the "Servers" area of the CMC, select the Adaptive Processing Server and go to **Manage > Properties**. In the **Command Line Parameters** field, enter the following command line parameter:

`-Dcom.businessobjects.publisher.threadpool.size=threadlimitnumber`

Replace *threadlimitnumber* with the thread limit number that you want.

If the publisher receives the error message

`java.lang.OutOfMemoryError: Java heap space` when you run a high-volume publication, it is because the Adaptive Processing Server has insufficient heap space. In the "Servers" area of the CMC, select the Adaptive Processing Server and go to **Manage > Properties**. In the **Command Line Parameters** field, change the number in the command-line parameter `-Xmx256m` to a larger number (for example, `-Xmx1024m`).

Note:

In some cases, you may have to create more instances of the Adaptive Processing Server to resolve “Out of memory” errors.

Working in high-volume publishing scenarios

In scenarios where Publications are sent to a high number of recipients with different profile values, the publishing resources may not be configured to take advantage of all the processing resources available in the deployment. Underemployed child job servers may actually cause performance bottlenecks through high volume requests to the system database.

It is possible to tune the Publishing Services to increase the number of simultaneously scheduled jobs by adjusting the `-Dcom.businessobjects.publisher.threadpool.size` property for the Adaptive Processing Server. Increasing the property will increase the use of available job (and children) servers.

Tip:

Some planning and testing in a development environment should be implemented before applying a new threadpool size to a production deployment.

Use the following guidelines when planning, testing and implementing a new value for the threadpool size property.

1. Do not use a threadpool size lower than 40.
2. Divide the target resource usage by the usage observed in high-volume publishing scenarios. Multiply the outcome by 40. Use this number as the target threadpool size. For example in a deployment running high volume publishing, 30% of the available job processing child servers are used to process jobs. If an administrator wants to increase utilization to 60%, the threadpool property value needs to be changed to 80
“-Dcom.businessobjects.publisher.threadpool.size=80”. This result is based on the calculation of 60% (target utility) divided by 30% (observed utility) multiplied by 40.

Note:

Increasing the threadpool property size impacts the memory used by the publishing resources and could impact other resources in the deployment. Adjusting the threadpool size property should therefore only be considered for high-volume publishing scenarios. Ensure that sufficient RAM is available and that the requisite memory is specified for the Adaptive Processing Server's Java memory settings.



Managing Auditing



12

chapter



This section provides an overview of the auditing functionality in BusinessObjects Enterprise. It also describes how to configure the auditing database, how to select actions to audit, and how to create a custom auditing report.

How does auditing work?

Auditing allows you to keep a record of significant events on BusinessObjects Enterprise servers (for a list of auditable events see the [Reference list of auditable events](#)). These records give you a picture of what information is being accessed, how it's being accessed, and who is looking at it.

For the purposes of this chapter, auditor refers to any system responsible for recording or storing information on any auditable event. Auditee refers to any system responsible for performing an event that is audited. There are some circumstances where a single system can be both an auditor and auditee. The Central Management Server (CMS) acts as the system auditor, while each BusinessObjects Enterprise server that controls events that you can monitor acts as an auditee.

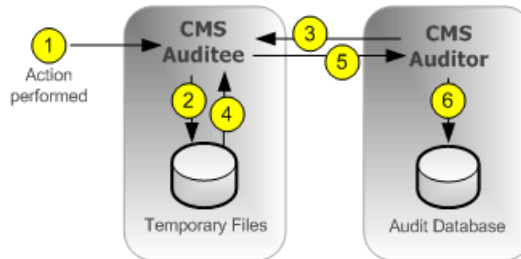
While the audit database can exist as part of the system database, it is recommended that it be kept separate, to minimize the impact on system performance due to the constantly growing size of the database. If you choose, you can use different database software for the CMS system database and the auditing database, and you can maintain these databases on separate servers. Once established, an auditing database is generally only appended to.

As the auditor, the CMS is responsible for collecting events and writing them to the auditing database. When an audited event is triggered, the server responsible will generate a record and store it in a local temporary file. At regular intervals the CMS communicates with the auditee servers to request copies of records from their local temporary files. When the CMS receives these records, it writes the data to the auditing database.

The CMS also controls the synchronization of auditing events that occur on different machines. Each auditee provides a time stamp for the auditing events that it records. To ensure that the time stamps 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 make a correction to the time they record for subsequent auditing events.

Depending on the type of client being audited, the system will use one of the following workflows to record the events.

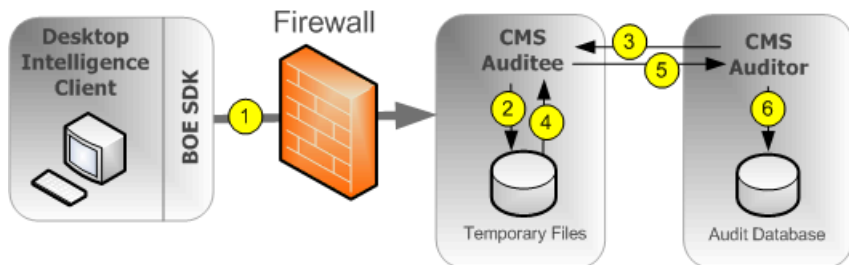
- Server auditing: This includes any automated operations that take place



NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

on a server.

1. An auditable event is performed by the server.
 2. The CMS-Auditee writes events in a temp file.
 3. CMS-Auditor polls CMS-Auditee periodically (every five minutes by default), and requests a batch of auditing events, (up to 200 by default).
 4. The CMS-Auditee retrieves the temp files.
 5. The CMS-Auditee transmits the events to the CMS-Auditor.
 6. CMS-Auditor writes events to the auditing database, and the CMS-Auditee then deletes the events from temp files.
- Client logon auditing for clients connecting through CORBA: This includes applications such as Desktop Intelligence or Web Intelligence Rich Client.



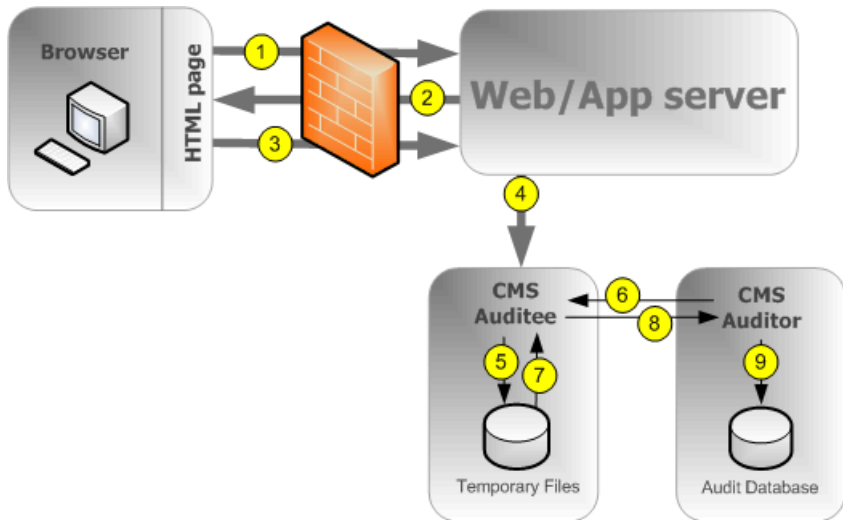
NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

1. The client connects to CMS-Auditee. The client provides its IP address and machine name, which the auditee then verifies.

Note:

A port should be opened in the firewall between the client CMS.

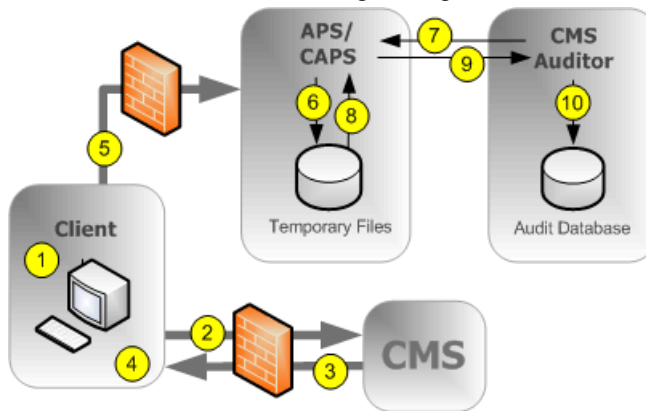
2. The CMS-Auditee writes events in a temp file.
 3. CMS-Auditor polls CMS-Auditee periodically (every five minutes by default), and requests a batch of auditing events, (up to 200 by default).
 4. The CMS-Auditee retrieves the temp files.
 5. The CMS-Auditee transmits the events to the CMS-Auditor.
 6. CMS-Auditor writes events to the auditing database, and the CMS-Auditee then deletes the events from temp files.
- Client logon auditing for clients connecting through HTTP: This includes online applications such as InfoView, Central Management Console, Desktop Intelligence ZABO client, Web Intelligence Rich Client, etc.



NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

1. The browser connects to the web application server.
2. The web application server returns main logon page.
3. The logon data is submitted to the web application server.
4. BusinessObjects SDK Enterprise submits logon request to the CMS auditee, along with the IP address and name of the browser machine. Enterprise SDK connects to CMS-Auditee, authentication is performed.
5. The CMS-auditee writes events in a temp file.
6. CMS-Auditor polls CMS-auditee periodically (every five minutes by default) and requests a batch of auditing events (up to 200 by default).
7. The CMS-Auditee retrieves the temp files.

8. CMS-Auditee sends events to the CMS-Auditor.
 9. CMS-Auditor writes events to the auditing database. CMS-Auditee deletes events from the temp files.
- Non-Logon auditing for clients connecting through CORBA: This workflow applies to auditing Desktop Intelligence client and Web Intelligence Rich Client events when connecting through CORBA.



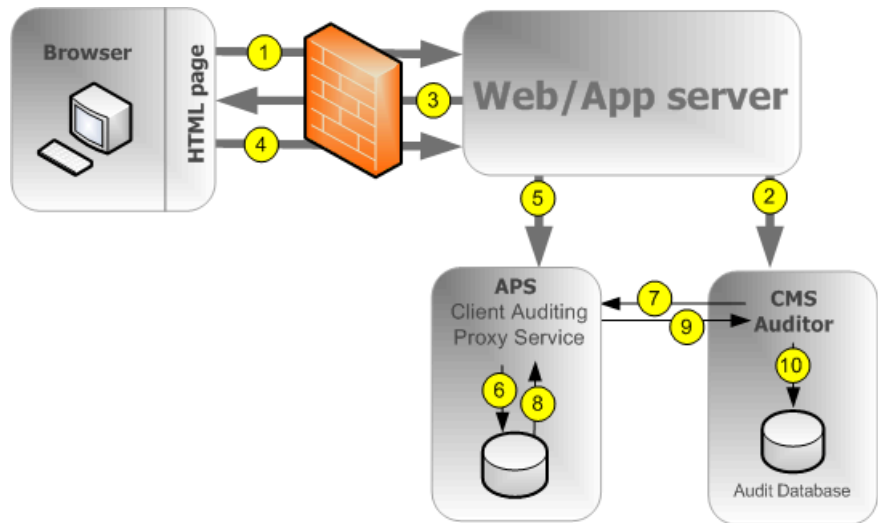
1. The user performs an operation that may be audited.
2. The client contacts the CMS to check if the operation needs to be audited.
3. The CMS informs the desktop client the operation requires auditing.
4. The client performs the operation.
5. The client sends the event information to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server.

Note:

A port in the firewall should be opened between each client and each Adaptive Processing Server.

6. CAPS writes events in a temp file.
 7. CMS-Auditor polls the CAPS periodically (every five minutes by default) and requests a batch of auditing events (200 by default).
 8. CAPS reads the temp file.
 9. CAPS sends the event information to the CMS-Auditor.
 10. CMS-Auditor writes the event information to the auditing database. CAPS deletes the events from the temp file.
- Non-login auditing for clients connecting through HTTP: This workflow applies to auditing Desktop Intelligence ZABO client and Web Intelligence

Rich Client events (except for logon events) when connecting through HTTP.



NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

1. The user initiates a potentially auditable event. The client application contacts the web application server.
2. The web application server contacts the CMS and checks to see if the event is configured to be audited.

Note:

While the diagram shows the Auditor CMS being contacted, 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. CAPS writes events in a temp file.
6. The CMS-Auditor polls the CAPS periodically (every five minutes by default) and requests a batch of auditing events (200 by default).
7. CAPS reads the temp file.
8. CAPS sends the event information to the CMS-Auditor.

9. CMS-Auditor writes the event information to the auditing database. CAPS deletes the events from the temp file.

Auditing consistency

Once the data is in the auditing database, you can run the auditing reports against the database or design custom reports to suit your business needs.

Note:

If you wish to remove a server from your BOE 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 post to the auditing database (the location of the temporary files is determined by the **Auditing Temporary Directory** setting on the CMC settings for that server). This may take several hours.

In most cases, where Auditing is properly installed, configured, secure, 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 Auditor database. While this delay is configurable, any of the following conditions may increase the delay beyond the configured limit.

- Unavailability of the CMS or auditing database.
- Loss of network connectivity.
- An auditee has generated more events than the CMS-Auditor is configured to retrieve in a single batch. See the links at the bottom of this page for instructions on increasing batch size.

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 that auditee servers always have plenty of disk space
- 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
- Deletion of auditee temporary files
- Hardware or disc 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 that don't support auditing.
- Transmission of auditing information may be blocked by improperly configured firewalls.

Related Topics

- [Optimizing system performance while auditing](#)

Configuring auditing

If you set up auditing when you installed BusinessObjects Enterprise, your auditing database is already configured and has established a connection with the Central Management Server (CMS). If you did not set up auditing when you installed, you must configure all your Server Intelligence Agent (SIA) to connect to an auditing database.

To be able to audit an event in BusinessObjects Enterprise, you will need to configure the following components:

- Determine which server controls the event (see [Reference list of auditable events](#)).
- You must enable auditing of that action in the Servers management area of the Central Management Console (CMC). For step by step instructions, see [Enabling auditing of user and system events](#).
- If it is a client-generated event, you must also enable auditing from the Applications area of the CMC. For step-by-step instructions, see [Enabling auditing of user and system events](#)

As the auditee, the BusinessObjects Enterprise server will then begin to trigger these auditing events in a local log file.

You can use any database server supported for the CMS system database for your auditing database. For a complete list of supported database software and version requirements see the BusinessObjects Enterprise supported platform document guide online on our support web site: http://support.businessobjects.com/documentation/supported_platforms.

If you plan to use MySQL for your auditing database, you will require version 3.51.12 of the MySQL Connector/ODBC (MyODBC) driver. If you do not

already have this installed, you can download it from the following location:
<http://dev.mysql.com/downloads/connector/odbc/3.51.html>.

It is recommended that you develop a back-up strategy for your auditing database. If necessary, contact your database administrator for more information.

If you have several servers of one type that you want to configure auditing on, you can use the configuration template to configure them identically. See the Working with Configuration Templates for more details.

Note:

- BusinessObjects Enterprise XI 3.1 will only audit events from client applications for 3.0 or higher; events from previous client versions will not be recorded. If you wish to audit events from all client applications they must be updated to BusinessObjects Enterprise XI 3.0 versions minimum.
- The CMS acts as both an auditor and auditee when you configure it to audit an action that the CMS itself controls.
- If you have a CMS cluster, every CMS in the cluster must be connected to the same auditing database, using the same connection method and the same connection name. Note that connection names are case sensitive.
- In a CMS cluster, the cluster will nominate one CMS to act as system auditor. If the machine that is running this CMS fails, another CMS from the cluster will take over and begin acting as auditor.
- The auditing database connections for all CMS servers should be identical (Database Host, DNS name, user ID and password should all be the same). If any of the connection details change then all nodes that host a CMS must be updated with this new information (through the Central Configuration Manager), or they will not be able to connect to the Auditing database.
- In order to ensure the highest degree of fault tolerance, it is recommended that you have more than one Adaptive Processing Server, each hosting a Client Auditing Proxy Service.
- Only one auditing database can be maintained for a cluster, and auditing reports cannot retrieve information across multiple auditing databases.

Related Topics

- [Clustering Central Management Servers](#)
- [Working with configuration templates](#)

Configuring auditing for servers on Windows

You will only need to configure your Windows servers if you did not install auditing when you installed BusinessObjects Enterprise. If you installed auditing, the servers will already be configured properly.

1. Open the CCM.
2. Stop the SIA.
3. Click **Specify Auditing Data Source**.

You will be prompted to select a database driver.

4. Specify whether you want to connect to the database through ODBC or through one of the native drivers.
5. Click **OK**.
6. The next step depends upon the connection type you selected:
 - If you selected ODBC, the Windows Select Data Source dialog box appears. Select the ODBC data source that you want to use as the auditing database and click **OK** (or click New to configure a new Data Source Name). Use a System DSN, and not a User DSN or File DSN. By default, the server is configured to run under the System account, which only recognizes System DSNs. When prompted, provide your database credentials and click **OK**.
 - If you selected a native driver, you are prompted for your database Server Name, your Login ID, and your Password. Provide this information and then click **OK**.
7. Click **OK**.
8. Start the Server Intelligence Agent. When the CMS starts it will populate the database with the required auditing tables.

Note:

You can also configure the auditing database using the Properties option for the SIA. Stop the agent, select **Properties**, and then go to the **Configuration** tab. Select **Write server auditing information to specified data source** and click **Specify**.

To configure the auditing database on UNIX

1. Use `ccm.sh` to stop the CMS.
2. Run `cmsdbsetup.sh`.
3. Choose the `selectaudit` option, and then supply the requested information about your database server.

Use `ccm.sh` to start the CMS. When the CMS starts, it will create the auditing database.

Which events can I audit?

You can audit the events of individual users of BusinessObjects Enterprise as they log in and out of the system, access data, or create file-based events. You can also monitor system events like the success or failure of scheduled objects. For each event, BusinessObjects Enterprise records the time of the event, the name and user group of the user who initiated the event, the server where it was performed, and a variety of other parameters more fully documented in [Reference list of auditable events](#).

Reference list of auditable events

This section contains the list of the auditable events you can enable in BusinessObjects Enterprise. It is organized according to the types of events that you can audit, to help you find the server where you enable auditing of these events.

If you are going to audit Publications you need to be aware of the following. As part of the publication process, BusinessObjects Enterprise creates temporary instance files for all recipients. If these events are being audited BusinessObjects Enterprise needs to maintain these instances, since they record details of the operation needed for the auditing process. This means the **Clean up instance after scheduling** option for Publishing will be ignored if these events are set as auditable.

Note:

- The following list of events is intended only to help you configure your system for auditing. It does not contain information on what event details are captured on these events.
- The list of auditable events for Desktop Intelligence and Web Intelligence Rich Client only apply when the client is actively logged in to BusinessObjects Enterprise. If the client is being use in an offline mode then events will not be recorded.

User events enabled on servers

The following table shows which server-based events can be audited and which server can be used to activate them.

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Objects	Object Created	CMS	CMS
	Object Deleted		
	Object Modified		
	Object Rights Modified		
	Unresponsive Scheduling		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Crystal re-ports	Report Viewing Succeeded	Crystal Reports Cache Service	Crystal Reports Cache Server
	Report Viewing Failed		
	Scheduling Succeeded	Destination Job Service	Destination Job Server
	Scheduling Failed		
	Scheduling Failed But Will Be Reat-tempted		
	Destination Delivery Succeeded		
	Destination delivery Failed		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Web Intelligence	<p>Document Retrieved</p> <ul style="list-style-type: none"> A user has saved a Web Intelligence document within BusinessObjects Enterprise. 	Web Intelligence Cache Service	Web Intelligence Cache Server
	<p>Universe Selected</p> <ul style="list-style-type: none"> A user has selected a universe as they create a new Web Intelligence document, or as they edit an existing Web Intelligence document. 		
	<p>Document Refreshed</p> <ul style="list-style-type: none"> User manually refreshes a Web Intelligence document, or opens a Web Intelligence document that is set to "refresh on open", or schedules a Web Intelligence document. 		
	<p>List Of Values Retrieved</p> <ul style="list-style-type: none"> A list of values is retrieved from the database to populate a pick-list associated with a prompt used to filter the data in a document. 		
	<p>Document Edited</p> <ul style="list-style-type: none"> User enters "Edit document" mode for an existing Web Intelligence document. 		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
	Format Applied <ul style="list-style-type: none"> User applies a formatting change to an existing Web Intelligence document in a query panel. 		
	SQL Generated <ul style="list-style-type: none"> This is triggered when a new Web Intelligence document is created. It then builds an SQL query for the document, but it is not submitted to the database. 		
	Drilled out of scope <ul style="list-style-type: none"> User drills past the scope of the data currently in memory, and triggers a call to the database for more data. 		
	Prompt Selected <ul style="list-style-type: none"> User enters or selects a value for a report prompt. 		
	Document Saved <ul style="list-style-type: none"> User opens an existing Web Intelligence document. 		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Web Intelligence scheduling and publishing	Scheduling Succeeded	Publishing Service	Adaptive Job Server
	Scheduling Failed		
	Scheduling Failed But Will Be Reattempted		
	Destination Delivery Succeeded		
	Destination Delivery Failed		
Desktop Intelligence scheduling and delivery	Scheduling Succeeded	Desktop Intelligence Job Service	Desktop Intelligence Job Server
	Scheduling Failed		
	Scheduling Failed But Will Be Reattempted		
	Destination Delivery Succeeded		
	Destination Delivery Failed		
	Document Retrieved <ul style="list-style-type: none"> User opens an existing Desktop Intelligence document. 		
	Document Refreshed <ul style="list-style-type: none"> User manually refreshes a Desktop Intelligence document, or opens a Desktop Intelligence document that is set to "refresh on open", or schedules a Desktop Intelligence document. 		
	Prompt Selected <ul style="list-style-type: none"> User enters or selects a value for a report prompt. 		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Desktop Intelligence documents	Document Retrieved <ul style="list-style-type: none"> User opens an existing Desktop Intelligence document. 	Desktop Intelligence Cache Service	Desktop Intelligence Cache Server
	Document Refreshed <ul style="list-style-type: none"> User manually refreshes a Desktop Intelligence document, or opens a Desktop Intelligence document that is set to "refresh on open", or schedules a Desktop Intelligence document. 		
	List of values Retrieved <ul style="list-style-type: none"> A list of values is retrieved from the database to populate a pick-list associated with a prompt used to filter the data in a document. 		
	Page Retrieved <ul style="list-style-type: none"> Server renders the pages of a Desktop Intelligence document in response to a user request to display all or part of a document. 		
	Prompt Selected <ul style="list-style-type: none"> User enters or selects a value for a report prompt. 		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Publication Scheduling	A job has been: <ul style="list-style-type: none"> successfully scheduled 	Publishing Job service	Publishing Job Server
	<ul style="list-style-type: none"> unsuccessfully scheduled 		
	<ul style="list-style-type: none"> unsuccessfully scheduled but will be reattempted 		
Replication	Scheduling Succeeded	Replication Service	Adaptive Job Server
	Scheduling Failed		
	Scheduling Failed But Will Be Reattempted		
Access levels	An access level has been created	CMS	CMS
	Custom access level modified		
	An access level has been deleted		
Users	Concurrent Logon	CMS	CMS
	Named User Logon		
	User Logon Failed		
	Password Changed		
	User Logoff		

Category	Event	BusinessObjects Enterprise Service	BusinessObjects Enterprise Server
Send an object to destination	Destination Delivery Succeeded (A user has successfully sent an object to a destination)	Destination Job Service	Destination Job Server
	Destination Delivery Failed (An object has failed to be sent to a destination)		
	Scheduling Failed But Will Be Reattempted		
File-based events	File Event Registered <ul style="list-style-type: none"> Event is created, and registered with system 	Event Service	Event Server
	File Event Updated <ul style="list-style-type: none"> The name, description, or file-name of an event is modified 		
	File Event Unregistered <ul style="list-style-type: none"> Event is removed from system 		
	File Event Triggered <ul style="list-style-type: none"> An event is triggered within the system 		

User events enabled for clients

The following table lists tells you which client-based events can be audited. Client events are set on the **Applications** section of the CMC. No modification of the client applications themselves is necessary.

Client	Events
Web Intelligence Rich Client events	Document Retrieved <ul style="list-style-type: none"> User opens an existing Web Intelligence document.
	Universe Selected <ul style="list-style-type: none"> A user has selected a universe as they create a new Web Intelligence document, or as they edit an existing Web Intelligence document.
	Document Refreshed <ul style="list-style-type: none"> User manually refreshes a Web Intelligence document, or opens a Web Intelligence document that is set to "refresh on open".
	List of Values Retrieved <ul style="list-style-type: none"> A list of values is retrieved from the database to populate a picklist associated with a prompt used to filter the data in a document.
	Document Edited <ul style="list-style-type: none"> User enters "Edit document" mode for an existing Web Intelligence document.
	Format Applied <ul style="list-style-type: none"> User applies a formatting change to an existing Web Intelligence document in a query panel.
	SQL Generated <ul style="list-style-type: none"> Server builds an SQL query for a Web Intelligence document (query is not submitted to DB).

Client	Events
	<p>Drilled out of scope</p> <ul style="list-style-type: none"> User drills past the scope of the data currently in memory, and triggers a call to the database for more data.
	<p>Prompt Selected</p> <ul style="list-style-type: none"> User enters or selects a value for a report prompt.
	<p>Document Saved</p> <ul style="list-style-type: none"> A user has saved a Web Intelligence document within BusinessObjects Enterprise.

Client	Events
Desktop Intelligence client events	Start Desktop Application (Three Tier)
	Document Retrieved <ul style="list-style-type: none"> User opens an existing Desktop Intelligence document.
	Document Refreshed <ul style="list-style-type: none"> User manually refreshes a Desktop Intelligence document, or opens a Web Intelligence document that is set to "refresh on open", or schedules a Web Intelligence document.
	Prompt Selected <ul style="list-style-type: none"> User enters or selects a value for a report prompt.
	List of Values Retrieved <ul style="list-style-type: none"> A list of values is retrieved from the database to populate a picklist associated with a prompt used to filter the data in a document.
	Universe List Retrieved
	Universe Selected <ul style="list-style-type: none"> A user has selected a universe as they create a new Desktop Intelligence document, or as they edit an existing Desktop Intelligence document.

Client	Events
	Document Edited <ul style="list-style-type: none"> User enters "Edit document" mode for an existing Web Intelligence document.
	Send to Users
	Document Saved

System events

	Event	BusinessObjects Enterprise Server
Scheduled objects	A job has been run successfully. For example, a scheduled Crystal report or publication has run successfully.	Job Servers
	<p>A job has failed to run. For example, a scheduled Crystal report or publication has failed to run.</p> <p>Tip: To auditing every failure of a scheduled Crystal report, a scheduled program, or a scheduled List of Values, enable auditing of "A job has failed to run" on the Job Server, and "Communication with a running instance is lost." on the Central Management Server.</p>	
	A job failed but will try to run again.	
	<p>Communication with a running instance is lost. For example, a scheduled Crystal report has failed to run because communication with the instance was lost, and the scheduled time for running the report expired.</p> <p>Note: You do not need to enable this option to auditing every failure of a scheduled Web Intelligence document.</p>	

Auditing and Publishing

You can audit actions related to Publishing with the sample report for Publishing that is included in BusinessObjects Enterprise. If you want to audit actions related to Publishing, keep these considerations in mind:

- You must configure auditing for every server used in the Publishing process. This includes destination servers, report job servers, and the publication job server.
- Publications intended for many recipients can generate many events that are recorded by the auditing database. Some of these events are related to the publication object, while other events are child events related to publication instances. The auditing database must have sufficient capacity to handle high-volume Publishing scenarios, or be configured to archive past actions.
- We recommend you turn on the **Object Deleted** event for all Central Management Servers.

Auditing information for publication destinations

The following table summarizes the information that an auditing report provides for each type of publication destination.

Destination type	Information provided in the auditing report
All destination types	<ul style="list-style-type: none"> • Publication name • Publication location in the CMS • File size • Delivery type (in this case, Publishing) • Reason for failure (if failure occurs) • Publication instance ID • Recipient name • Document scope (for personalization)
Email	<ul style="list-style-type: none"> • Domain name • SMTP server • Port • From, To, and CC addresses • Attachment file name
FTP server	<ul style="list-style-type: none"> • FTP host name • Port • FTP user name • File path
Local disk	<ul style="list-style-type: none"> • File path
InfoView inbox	<ul style="list-style-type: none"> • Recipients' user names
Printer	<ul style="list-style-type: none"> • Printer name • Name and path for each document printed • Number of copies <p>Note: This feature is available for Crystal reports only.</p>

Enabling auditing of user and system events

After you determine which BusinessObjects Enterprise server controls the event, you must enable auditing on the server from the Servers management area of the Central Management Console (CMC).

If you have multiple BusinessObjects Enterprise servers of a given type, be sure to enable identical auditing events on every server. This ensures you collect information on all user or system events in your BusinessObjects Enterprise system. For example, if you are interested in the total number of concurrent user logons, enable auditing of concurrent user logons on each of your Central Management Servers. If you enable auditing on only one Central Management Server, you will only collect auditing information about events that occur on that server.

In some special cases you may wish to enable auditing on only one server of a given type. For example, if you are interested in the success or failure of only one kind of scheduled report and you have configured your system so that these reports are processed on one particular Job Server, it is not necessary to enable auditing on every Job Server in your system. You only need to enable auditing on the Job Server where the reports are processed.

Note:

You must configure the auditing database before you can collect data on auditing events. See [Configuring auditing](#) for information on how to configure the auditing database.

When you are configuring auditing on you system, you can use the **Configuration Template** option to apply settings across multiple servers of the same type. One of the advantages to this method is that it allows you to apply changes to all your auditee servers of a particular type from a single location. See [Working with configuration templates](#).

Note:

For auditing Desktop Intelligence client and Web Intelligence Rich Client events, you must also configure the these applications in the CMC.

To enable auditing events on servers

1. Go to the **Servers** area of CMC.
2. Click the server that controls the action that you wish to audit.
(See the [Reference list of auditable events](#) to find the correct server.)
3. Click **Actions > Audit Events** .

The "Audit Events" options will be displayed.

4. If you are using a temporary file directory other than the default, enter the path to the directory in **Auditing Temporary Directory**.
5. In **Events per file** enter the maximum number of audit events you want stored in the temporary file.

Note:

If this number of events is exceeded, then these events will be split over multiple files. See [Optimizing system performance while auditing](#).

6. Click **Auditing is enabled**.
7. Under the "Select Events to Audit" section, select the auditing events that you wish to record.
8. Click **Save & Close**.

Tip:

To audit every failure of a scheduled Crystal report, a scheduled program, or a scheduled List of Values, enable auditing of "Scheduling Failed" on the Job Server the Central Management Server.

Note:

- We recommend that you turn on the **Object Deleted** auditing event on all CMS servers if you are enabling auditing.
- In some cases you may also want to select the **Disable Auto Reconnect to System and Auditing Databases** (on the CMS "Properties" page in CMC). In the event of a power failure, or other service disruption, this allows administrators to check the integrity of the auditing database before resuming operations. No auditing events will be lost, as they will continue to reside in the temporary files on the appropriate servers until reconnection with the CMS can be established.
- Ensure that your auditing log file is located on a hard drive that has sufficient space to store the temporary files. (See [Optimizing system performance while auditing](#) for information on adjusting the size of temporary files.)
- [Which events can I audit?](#)
- [Using sample auditing reports](#)

To enable auditing events for client applications

In order to audit client events, your BusinessObjects Enterprise deployment must have the following in place.

- You will need at least one Adaptive Processing Server with Client Auditing Proxy Service and auditing enabled on this server.
 - For clients connecting through CORBA, you must open a port in the firewall between the client and the Adaptive Processing Server machines.
 - For client connection through HTTP (Desktop Intelligence ZABO client, Web Intelligence Rich Client, InfoView, etc.), you must open a port in the firewall between the Web Application Server and the Adaptive Processing Server machines.
 - Auditing must be enabled on the Cache and Job servers for Desktop Intelligence or Web Intelligence (or both).
1. Go to the **Applications** area of the CMC.
 2. Click the application that controls the action you wish to audit.
 3. Click **Actions > Audit Events**.
The "Audit events" screen is displayed.
 4. Click **Auditing Status**.
 5. Under the **Check events you want to audit** section, select the auditing events that you wish to record.
 6. Click **Update**.

Auditing Configuration Template

The configuration template allows you to easily modify the settings on several servers. The settings you enter for the template can be applied to all the selected servers in your deployment.

By default the configuration template will be configured with the auditing settings specified during your BusinessObjects Enterprise installation (the install default is to have auditing disabled). You can modify the template at any time by accessing the Auditing settings for any Auditee server in your deployment.

There are two ways to see the current settings of the configuration template. The simplest way is to view the Auditing settings on one of the servers you

know uses the template. The settings will appear (grayed out) on that page. Alternatively you can set one of the Auditee servers to use the template, and save that change. The configuration template's settings will then be visible on the Auditing settings page.

Configuration templates can also be used for functions other than auditing. For more details, see [Working with configuration templates](#).

To set the Configuration template

1. Go to the servers area of the CMC
2. Double click one of the servers you wish to configure using the configuration template.
3. Click **Auditing Events**.
The "Auditing Configuration" page is displayed.
4. If **Use Configuration Template** is already set, uncheck it.
5. Configure the Auditing settings according to your preferences.

Note:

The Auditing events are not part of the Configuration Template.

6. Click **Set Configuration Template**.
7. Click **Save & Close**.

The settings on this page will be applied to all the servers that have **Use configuration template** set for Auditing. The applies to all server types.

You can apply the Configuration Template to any auditee server by accessing its Auditing settings and clicking **Use configuration template**.

Note:

- Once you have set the configuration template, we recommend that you uncheck **Set Configuration Template** and set **Use Configuration Template** on the server you used to configure the template. This prevents users for accidentally modifying the template by changing the settings for that server.
- If you uncheck **Use Configuration Template** on a server, all the Auditing settings will remain in their current state until you enter new information. The server will not revert to its original settings.

Configuring the universe connection

The auditing reports use the Activity universe. Before you can view these reports, you must configure the universe connection. If you installed auditing when you set up and configured your BusinessObjects Enterprise, this connection will already be configured.

If you did not install auditing when you set up BusinessObjects Enterprise, you will need to configure this connection before you view auditing reports. This involves two steps: first you must create a data source for your auditing database (unless you have a native connection you plan to use), next you must specify this data source for your universe connection.

Note:

For Windows systems you may need to create an ODBC system DSN to point to your audit database.

To configure the Activity universe connection

Note:

This will configure the Activity universe that the sample reports are designed to run against. If you are using custom reports you will need to connect to the universe that those reports are designed for.

1. Start the Designer application and logon to your CMS.
2. Close the "Quick Design Wizard" if it opens.
3. Click **File > Import**.
The "Import Universe" window opens.
4. Select **Browse** and choose the root folder, then click **OK**.
A list of universes is displayed.
5. Select the "Activity" universe and click **OK**, then click **OK** again.
A message is displayed, saying that the universe was successfully imported.
6. Click **OK**.
7. From the menu bar, click **File > Parameters**.
The "Universe Parameters" window opens.
8. Click **New** to start the New Connection Wizard, then click **Next**.

9. Type in any name into the Connection Name field and select the Data Access Driver for your connection. Specify your user name, password, and data source, alias, or service name. Click **Next** twice, then click **Finish**.
10. Click **File** > **Save** to save the connection you have created.
11. Click **File** > **Export**.
The "Export Universe" window opens.
12. In the Domain field, select the location you imported the Activity universe from and click **OK**.
A message is displayed, saying that the universe was successfully exported.
13. Click **OK** and exit the "Designer" application.

Using sample auditing reports

BusinessObjects Enterprise includes two sets of sample auditing reports:

- One set was created using Crystal Reports.
- One set was created using Web Intelligence.

Both sets of reports are available in the sample folder on your product distribution in the file `auditing.biar`.

These sample reports are published to the Auditor folder when you install BusinessObjects Enterprise with a product keycode which authorizes you to use Auditor. The Crystal Reports auditing reports are available as object packages with the report sections as individual documents. The Web Intelligence auditing reports are available as Web Intelligence documents with the report sections as tabs within the documents. Both sets of reports are based on the Activity universe.

Note:

You can also deploy the auditing reports to another cluster. To do this, use the Import Wizard to deploy the `auditing.biar` to the CMS on the node where you want the reports. For further details, see the Import Wizard help.

Note:

Current auditing reports are designed to run from a single auditing database.

If you configured the auditing database when you installed BusinessObjects Enterprise, you must enable the auditing of the user and server actions. For

information on how to enable auditing on servers, see [Enabling auditing of user and system events](#).

If you did not configure the database when you installed BusinessObjects Enterprise, before you use the reports, you must do the following:

- Configure the auditing database before you use the sample reports.

For information on how to configure the auditing database, see [Configuring auditing](#)

- Enable the auditing of the user and server actions needed to provide data for the sample reports.

For information on how to enable auditing on servers, see [Enabling auditing of user and system events](#)

- Configure the universe connection used for the sample reports.

For procedural details, see [Configuring the universe connection](#).

After you enable auditing of the user and server actions, the auditing database will then begin to be populated with the auditing data you specified.

Note:

If you have recently enabled auditing, the sample auditing reports may contain little or no data the first time you view them.

Controlling synchronization of auditing actions

The CMS controls the synchronization of auditing actions that occur on different machines. The CMS periodically broadcasts its system time to the auditees in UTC (Coordinated Universal Time). The auditees compare this time to their internal clocks, and then make the appropriate correction to the time stamp (in UTC) they record for subsequent auditing actions. This correction affects only the time stamp that the auditee records in its auditing log file. The auditee does not adjust the system time of the machine on which it is running.

By default, the CMS broadcasts its system time every 60 minutes. You can change the interval using the CMS command-line option:

```
-AuditeeTimeSyncInterval minutes
```


You can turn off this option by setting `minutes` to zero. For more information on the CMS, see the Server Command Lines chapter in the *SAP BusinessObjects Enterprise Administrator's Guide*.

This built-in method of time synchronization will be accurate enough for most applications. For more accurate and robust time synchronization, configure the auditee and auditor machines to use an Network Time Protocol (NTP) client, and then turn off internal synchronization by setting:

```
-AuditeeTimeSyncInterval 0
```

Tip:

If you have a CMS cluster, apply the same command-line options to each server. Only one CMS in the cluster acts as the auditor. However, if this CMS fails, another CMS takes over auditing. This CMS will apply its own command-line options. If these options are different from those of the original auditor, auditing behavior may not be what you expect.

Optimizing system performance while auditing

Enabling auditing can effect on the performance of BusinessObjects Enterprise. However, you can optimize system performance by fine-tuning these options:

- **AuditInterval** `minutes`, where `minutes` is between 1 and 15. (The default value is 5.) The CMS requests auditing records from each audited server every auditing interval.
- **auditMaxEventsPerFile** `number` (`number` has a default value of 500 and must be greater than 0). The maximum number of records that an audited server will store in a single auditing temp file. When this maximum value is exceeded, the server opens a new temp file.

Note:

Temp files remain on the audited server until all records have been requested by the CMS.

Changing each of these options has a different impact on system performance. For example, increasing the auditing interval reduces frequency with which the CMS writes events to the auditing database. Decreasing the audit interval increases the rate at which records are moved from the auditing temporary files on the audited servers to the auditing database, thereby

decreasing the length of time that it takes these records to get transferred to the central auditing database. Increasing the maximum number of auditing events stored in each auditing log file reduces the number of file open and close operations performed by audited servers.

You can use these options to optimize auditing performance to meet your needs. For example, if you frequently need up-to-date information about audited events, you can choose a short auditing interval and a large temporary file size. In this case, all auditing records are quickly transferred to the auditing database, and you can always report accurately on the latest audited events. However, choosing these options may have an impact on the performance of BusinessObjects Enterprise.

Alternatively, you may only need to review auditing results periodically (weekly, for example). In this case you can choose to increase the auditing interval, and to decrease the number of auditing records in each batch. Choosing these options minimizes the impact that auditing has on the performance of BusinessObjects Enterprise. However, depending upon activity levels in your system, these options can create a backlog of records stored in auditing temporary files. This backlog is cleared at times of low system activity (such as overnight, or over a weekend), but means that at times your auditing reports may not contain records of the most recent audited events.



Auditing Reports

13

chapter



Using auditing reports

If you are an administrator who wants to view reports from the auditing database, you have these choices:

- You can use the auditing reports that are included with BusinessObjects Enterprise.
- You can modify the auditing reports that are included with BusinessObjects Enterprise.
- You can create your own auditing reports.

Why are reports important?

Auditor includes reports that can answer questions you may have about your BusinessObjects Enterprise deployment. Each report contains one or more report sections that focus on a very specific area.

Table 13-1: Questions Auditing can answer

Category	Question	Report
User Information	How many users are on my system?	Average Number of Users Logged In
	What is the average session duration?	Average Session Duration
	What is the average session duration per user?	Average Session Duration per User
	From where are users logging into my system?	IP Addresses Accessing My Cluster
	How many jobs were processed per user?	Jobs per User
	When was the last time a specific user used the system?	Last Login for User
	Who is using the system the most? (by refresh or by login)	Most Active Users
	Number of logged in sessions	Number of User Sessions
	How many users have used the system?	Number of Users in the System
	Whose passwords have been modified?	Password Modifications
	Who does not log out correctly?	Users Who Logged Off Incorrectly

Category	Question	Report
Document Information	What is the average time for documents to refresh?	Average Refresh Time
	Document Usage Analysis	Document Information Detail
	How often have documents been scheduled and viewed?	Document Scheduling and Viewing Status
	What are the 10 least viewed, edited, and refreshed documents?	Least Accessed Documents
	What are the 10 most viewed, edited, and refreshed documents?	Most Accessed Documents
	What are the most popular actions per document?	Most Popular Actions per Document
	How often has an operation been performed on a document?	Operations on Documents
	How often have documents been published?	Publishing Auditing
System Information	What is the average session duration per cluster?	Average Session Duration per Cluster
	How many Job Services do I have?	Job Services on the System
	How many jobs are there?	Job Summary
	How many jobs were processed per Job Service?	Jobs per Job Service Type
	How many audited servers do I have?	Services in the Cluster

Category	Question	Report
Impact Analysis	What are the most popular actions?	Most Popular Actions
	How many users are accessing my system daily and when is the most popular time?	Peak Usage
	Are my users editing reports or only refreshing them?	Refresh and Edit Activity
	What objects have had their rights changed?	Rights Modification
	How many users are on my system?	Total Users Logged In by Day
	What is my users activity by month, week, day?	User Activity
	What do the users do?	User Activity per Session

Auditing report names

This section contains the following:

- the list of the report names
- the report sections included with the reports
- the report prompts

Note:

Folder path prompts will not automatically include objects/documents in subfolders below the selected folder. For example, selecting the folder `toplevel` will show results for all documents in the `toplevel` folder, but not for any objects/documents in the `toplevel/sublevel` folder. To see objects/documents in all subfolders, enter `toplevel%`.

Average Number of Users Logged In

The average number of sessions and users logging in over a given period of time.

Report sections	Report prompts
Average Number of Sessions	Select a start and end date.
Users Logged In	
Average Number of Users Logged In	

Average Refresh Time

The average refresh time per document, user, or cluster over the specified time period.

Report sections	Report prompts
Average Refresh Time by Document	Enter a folder path and document type, select a start and end date.
Average Refresh Time by User	
Average Refresh Time by Server	

Average Session Duration

The average duration of user sessions, broken down by year, quarter, month, week, day, or hour.

Report sections	Report prompts
Year	Enter User name, select a start and end date.
Quarter	
Month	
Week	

Report sections	Report prompts
Day	
Hour	

Average Session Duration per Cluster

The average duration of sessions for a cluster of servers, by year, month, week, or day.

Report sections	Report prompts
Average Session Duration in Minutes per Year	Select a start and end date.
Average Session Duration in Minutes per Month	
Average Session Duration in Minutes per Week	
Average Session Duration in Minutes per Day	

Average Session Duration per User

The average duration of specific users' sessions, by year, month or week.

Report sections	Report prompts
Average Session Duration in Minutes over the Year	Select a start and end date.
Average Session Duration in Minutes per Month per User	
Average Session Duration in Minutes per Week per User	

Cluster Nodes

The names of all servers in the audit cluster.

Report sections	Report prompts
Servers in the Cluster	None

Document Information Detail

Provides details of actions performed on a given document.

Report sections	Report prompts
Document Information	Enter document name and folder path, select a start and end date.

Document Scheduling and Viewing Status

The status of document jobs and views over a specified period of time.

Report sections	Report prompts
Scheduleing Status	Enter folder path, select start and end date.
Crystal Reports Viewing Status	
Web Intelligence Viewing Status	
Desktop Intelligence Viewing Status	

IP Addresses Accessing My auditing Clusters

The IP addresses or machine names of clients accessing the audit cluster.

Report sections	Report prompts
IP Addresses Accessing My auditing Clusters by IP - Day	Select start and end date.
IP Addresses Accessing My auditing Clusters by IP - Month	
IP Addresses Accessing My auditing Clusters by Name - Day	
IP Addresses Accessing My auditing Clusters by Name - Month	

Jobs per Job Service

Number of jobs per server type, kind, or specific server.

Report sections	Report prompts
Jobs per Job Server Kind- Summary	None
Jobs per Job Server Kind	
Jobs per Job Service	

Job Services on System

Number of job services on the system, and the duration of any jobs in seconds (optional).

Report sections	Report prompts
Job Services	None
Job Services and Duration of Jobs (sec)	

Job Summary

Number of jobs on the system by status, or number of successfully completed or failed jobs over a given period.

Report sections	Report prompts
Jobs per Status	Enter folder path, select start and end date.
Successful Jobs	
Failed Jobs	

Jobs per User

A summary of the number of jobs and their durations a user has initiated over a given period of time.

Report sections	Report prompts
Jobs per User - Summary	Select start and end date.
Jobs per User	
Job Duration per User	
Job Failures per User	

Last Login for User

Last date and time to the second that a given user logged in to the system.

Report sections	Report prompts
Last Login for User	Enter User name, select start and end date.

Least Accessed Documents

Identifies the least popular documents by times read, edited or refreshed over a given period.

Note:

Documents that are never accessed it will not generate any events and not show up as part of this report.

Report sections	Report prompts
Least Accessed Documents - By times Read	Select document type and enter folder path, select start and end date.
Least Accessed Documents - By Edits	
Least Accessed Documents - By Re-freshes	

Most Accessed Documents

Most used documents based on times read, edited or refreshed over a given period.

Report sections	Report prompts
Most Accessed Documents - By times Read	None
Most Accessed Documents - By Edits	
Most Accessed Documents - By Re-freshes	

Most Active Users

A list of the system's most active users over a given period of time.

Report sections	Report prompts
Most Active Users by Logins	Select start and end date.
Most Active Users by Refreshes	

Most Popular Actions

Quantity of the most popular actions during a given time period

Report Sections	Report Prompts
Most Popular Actions per Year	Select start and end date.
Most Popular Actions per Quarter	
Most Popular Actions per Month	
Most Popular Actions per Week	
Most Popular Actions per Day	

Most Popular Actions per Document

Quantity of the most popular actions for a specified document during a given time period or by specified user.

Report sections	Report prompts
Most Popular Actions per Document-By User	Select document name and enter folder path, select start and end date.
Most Popular Actions per Document-By Session	
Most Popular Actions per Document-By Action	
Most Popular Actions per Document-By Month	

Number of User Sessions

Total number of user sessions for a cluster organized per year, month, week, and day.

Report sections	Report prompts
by Month	Select start and end date.
by Week	
by Day	

Number of Users in the System

The number of users in the system at the time the report is run.

Report sections	Report prompts
Number of Users in the System - Active Users	None

Operation on Documents

The types of operations performed on specified documents, by time, type, user and document, or user.

Note:

Only document types that have generated auditing events will appear in the **Document Type** prompt dropdown.

Report sections	Report prompts
Operation on Documents - By Time	Enter user name, Document type and folder path, select operation and start and end date.
Operation on Documents - By Operation Type	
Operation on Documents - By User and Document	
Operation on Documents - By User	

Password Modifications

A summary of password modification operations over a specified period of time.

Report sections	Report prompts
Password Modifications - By Month	Select start and end date.
Password Modifications - By Week	
Password Modifications - By Details	

Peak Usage

Charts the peaks of user logins, session logins or number of actions performed over a given period of time.

Report sections	Report prompts
Users Login Peaks	Select start and end date.
Session Login Peaks	
Number of Action Peaks	

Publishing auditing

Publication activity for a specific document over a given period of time.

Report sections	Report prompts
Publishing Auditing	Enter publication name, select start and end date.

Refresh and Edit Activity

Number of edit and refresh actions per document trace, per cluster, and per selected user over a given period.

Report sections	Report prompts
Refresh and Edit Activities of Web Intelligence Documents	Select user name, document name and folder path, select start and end date.

Rights Modification

A summary of security activities for a specified folder over a given period of time.

Report sections	Report prompts
Rights Modification - By User	Select folder path, select start and end date.
Rights Modification - By Object	

Services in the Cluster

Report sections	Report prompts
Services in the Cluster	None.

Total Users Logged In by Day

A summary of the number of users or sessions logged in over a given time period, broken down by day.

Report sections	Report prompts
Total Users Logged In by Day -Total Number of Logged In Users	Select start and end date.
Total Users Logged In by Day - Total Number of Logged in Sessions	

User Activity

Number of users using the system per month, week, or day within a given time period.

Report sections	Report prompts
User Activity by Month	Select start and end date.
User Activity by Week	
User Activity by Day	

User Activity per Session

Analyses user activity for the whole content of the audit database per cluster, session, action, or date.

Report sections	Report prompts
User Activity per Session Per Cluster	Enter user name, select start and end date.
User Activity per Session Per Session	
User Activity per Session Per Action Name	
User Activity per Session Per Date	

Users Who Logged Off Incorrectly

Of the users who logged in during a given period, which ones failed to log off correctly.

Report sections	Report prompts
Statistics	Select start and end date.
Users Who Logged Off Incorrectly	

Viewing sample auditing reports

To view sample auditing reports

1. Log on to InfoView.
2. Click **Public Folders**.
3. Click **Auditing Reports**.
4. Click the language folder of your choice.
A list of sample auditing reports is displayed.
5. Open the report you want to view.
 - To open a Web Intelligence auditing report, click on the report you want to view.

- To open a Crystal Reports auditing report, open the object package, and then open the report you want to view.

Creating custom auditing reports

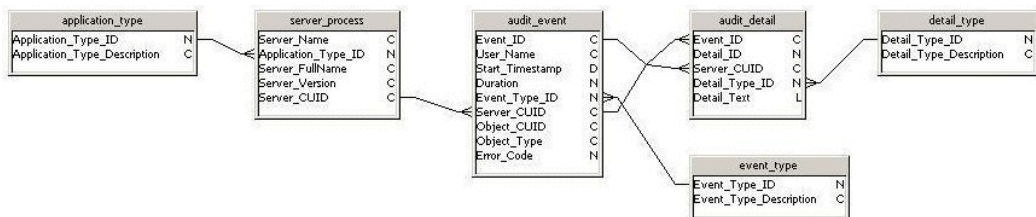
This section contains information to help you understand the auditing database, the Activity universe and the information it records about auditing actions. With this information, you can use Crystal Reports, Web Intelligence or Desktop Intelligence to create custom auditing reports of user and system actions.

Auditing database schema reference

The auditing database contains six tables:

- [Audit_Event](#)
- [Audit_Detail](#)
- [Server_Process](#)
- [Detail_Type tables](#)
- [Event_Type](#)
- [Application_Type](#)

The following diagram shows the schema of the auditing database.



Audit_Event

The `Audit_Event` table stores one record per action that is audited and contains general information about each auditing event.

Field	Description
Server_CUID	Server and service ID. Combined with the Event_ID to form the primary key for the Audit_Event table.
Event_ID	A unique ID generated by the server to identify the auditing event. Combined with Server_CUID to form the primary key for the Audit_Event table.
User_Name	Name of user who performed the action.
Start_TimeStamp	Time for start of action in UTC (Coordinated Universal Time) to the nearest millisecond. The time stamp is created by the server recording the action in its log file, and includes any correction necessary to synchronize with CMS time. You may want to correct this time to your local time zone when creating auditing reports.
Duration	Duration, in seconds, of the action that is audited.
Event_Type_ID	Number that uniquely identifies the type of action the entry represents. Foreign key for the Event_Type table.
Object_CUID	Info Object CUID of object associated with the action. This number uniquely identifies an object such as a document, folder or user.
Object_Type	Identifies the program that initiates the action, such as Web Intelligence, Desktop Intelligence, Crystal Reports, or Voyager.
Error_Code	Field reserved for error codes.

Audit_Detail

The `Audit_Detail` table records more details about each auditing action recorded in the `Audit_Event` table. For example, when a user logon fails, the reasons for that failure are recorded as auditing details.

There may be more than one record in this table for each auditing action recorded in the `Audit_Event` table.

Field	Description
<code>Server_CUID</code>	Combination of the Server and Service CUID responsible for the event. Combined with the <code>Event_ID</code> and the <code>Detail_ID</code> to form the primary key for the <code>Audit_Detail</code> table.
<code>Event_ID</code>	A unique ID generated by the server to identify the auditing event. Combined with <code>Server_CUID</code> and the <code>Detail_ID</code> to form the primary key for the <code>Audit_Detail</code> table.
<code>Detail_ID</code>	The <code>Detail_ID</code> field is used to number the individual details associated with each auditing action (i.e. if there are two details associated with a particular auditing action, the first will have a <code>Detail_ID</code> of 1, and the second will have a <code>Detail_ID</code> of 2).
<code>Detail_Type_ID</code>	Number that uniquely identifies the type of detail about the auditing action that the entry represents. Foreign key for the <code>Detail_Type</code> table.
<code>Detail_Text</code>	Information about the auditing detail being recorded. For example, if the <code>Detail_Type_Description</code> were "universe name", the detail text would contain the name of that universe.

Server_Process

The `Server_Process` table contains information about the servers and services running within your BusinessObjects Enterprise system which can generate auditing events.

Field	Description
Server_CUID	Combination of the Server and Service CUID of the server InfoObject that created the event. Primary key for the <code>Server_Process</code> table.
Server_Name	Machine name of the server that produced the action. That is, the host name.
Application_Type_ID	A unique ID that identifies the type of application that generated the auditing action. Foreign key to the <code>Application_Type</code> table.
Server_FullName	Name of the server and service that initiated the action. The names are the same as those displayed in the CMC. The default name is <i>host name.servertype</i> .
Server_Version	Version of BusinessObjects Enterprise on server that produced the action.

Event_Type

The `Event_Type` table contains a static list of the kinds of events that can be audited in your BusinessObjects Enterprise system. This table provides information roughly equivalent to that provided by AuditIDs and AuditStrings in Crystal Enterprise

Field	Description
Event_Type_ID	Number that uniquely identifies the type of auditing event that the entry represents.

Field	Description
Event_Type_Description	Description of the type of auditing event.

Application_Type

The `Application_Type` table contains a static list of the applications that can produce auditing events.

Field Name	Description
Application_Type_ID	A unique ID that identifies the type of application that generated the auditing action.
Application_Type_Description	The description of the application generating the auditing event.

Detail_Type tables

The `Detail_Type` table contains a static list of the standard details that can be recorded about audited events. For example, a user logon can fail for a number of different reasons. These reasons are listed as entries in the `Detail_Type` table.

The information in the `Detail_Type` table is equivalent to the information that was recorded in variable `AuditStrings` in Crystal Enterprise 10.

Field	Description
Detail_Type_ID	Number that uniquely identifies the type of auditing detail that the entry represents.

Field	Description
Detail_Type_Description	The description of the type of auditing detail generated by the auditing event.

Event and Detail reference tables

The following tables list the `Event_Type_ID` and `Event_Type_Description` of all events that can be audited in your system. For your convenience, these events are ordered according to the service that generates each type of event.

The following table shows an example event.

Event ID	Event Description	Detail ID	Detail Description	Detail Text
65537	Concurrent user login succeeded.	42	User Groups	Admin
65537	Concurrent user login succeeded.	45	Session ID	1234
65537	Concurrent user login succeeded.	60	IP address reported by client	123.456.101.100
65537	Concurrent user login succeeded.	61	Hostname reported by client	host.domain.com
65537	Concurrent user login succeeded.	62	IP address resolved by server	123.456.101.100
65537	Concurrent user login succeeded.	63	Hostname resolved by server	host.domain.com

Event ID	Event Description	Detail ID	Detail Description	Detail Text
65537	Concurrent user logon succeeded.	89	Concurrent user account	juser

The following tables list the Event_Type_ID code for the event, the description, and any details that will be associated with that event followed by their Detail_ID codes in parenthesis.

CMS auditing events

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
65537	Concurrent user logon succeeded.	<ul style="list-style-type: none"> • Concurrent User Count (89) • Hostname reported by client (61) • Hostname resolved by server (63) • IP address reported by client (60) • IP Address resolved by server (62) • Session ID (45) • User Groups (42)
65538	Named user logon succeeded.	<ul style="list-style-type: none"> • Concurrent User Count (89) • Hostname reported by client (61) • Hostname resolved by server (63) • IP address reported by client (60) • IP address resolved by server (62) • Session ID (45) • User Groups (42)
65540	User logged off.	<ul style="list-style-type: none"> • Concurrent User Count (89) • Session ID (45) • User Groups (42)
65541	User password has been changed.	<ul style="list-style-type: none"> • Session ID (45) • User Groups (42)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
65539	User logon failed.	<ul style="list-style-type: none">Enterprise Error Text (46)Hostname reported by client (61)Hostname resolved by server (63)IP address reported by client (60)IP address resolved by server (62)Logon using token (64)User Groups (42)
65542	Object created.	<ul style="list-style-type: none">Object CUID (92)Object Folder Path (43)Object instance (90)Object Name (3)Object Type (50)Parent Document CUID (91)Session ID (45)User Groups (42) <p>Note: This auditing string will not be recorded when a new user account is created, even though a new folder is created for each new user.</p>
65543	Object deleted.	<ul style="list-style-type: none">Object Folder Path (43)Object instance (90)Object Name (3)Object Type (50)Session ID (45)User Groups (42)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
65544	Object modified.	<ul style="list-style-type: none"> Object CUID (92) Object Folder Path (43) Object instance (90) Object Name (3) Object Type (50) Parent Document CUID (91) Session ID (45) User Groups (42)
65545	Unresponsive scheduling.	
65546	Object Rights Modified	<ul style="list-style-type: none"> Object Folder Path (43) Object instance (90) Object Name (3) Object Type (50) Parent Document CUID (91) Session ID (45) User Groups (42)

Cache service auditing events

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
196609	Report Viewing Succeeded.	<ul style="list-style-type: none"> Object Folder Path (43) Object instance (90) Object Name (3) Parent Document CUID (91) Report Data Type (51) User Groups (42)
196610	Report Viewing Failed.	<ul style="list-style-type: none"> Enterprise Error Text (46) Object Folder Path (43) Object instance (90) Object Name (3) User Groups (42)

Job service auditing events

For scheduled objects (by clients or servers), the auditing messages give you information about the status of scheduled actions. For example, the auditing messages can tell you if a scheduled report ran successfully.

For the Destination Job service, the auditing messages give you information on whether an object was sent to a destination, as requested by a user.

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
327681	Job successful.	<ul style="list-style-type: none"> • Object Folder Path (43) • Object instance (90) • Object Name (3) • Parent Document CUID (91) • Universe name (2) • User Groups (42)
327682	Job failed.	<ul style="list-style-type: none"> • Object Folder Path (43) • Object instance (90) • Object Name (3) • Parent Document CUID (91) • Universe name (2) • User Groups (42)
327683	Job failed. Job will be retried by the CMS.	<ul style="list-style-type: none"> • Object CUID (92) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Template Document (91) • Universe Name (2) • User Groups (42) <p>Note: For more information on scheduling jobs, see the <i>SAP BusinessObjects Enterprise Administrator's Guide</i>.</p>

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
327687	Destination Delivery Succeeded	<ul style="list-style-type: none"> • Destination Delivery Type (66) • Destination Type (65) • Document Scope (81) • Document size (9) • Domain (71) • File Name (68) • From Address (73) • Host Name (70) • Object CUID (92) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Port (72) • Publication Instance ID (82) • Recipient Name (80) • Template Document CUID (91) • To Address (74) • User Groups (42) • User Name (69)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
327688	Destination Delivery Failed	<ul style="list-style-type: none"> • Destination Delivery Type (66) • Destination Type (65) • Document Scope (81) • Document size (9) • Domain (71) • Error Message (76) • File Name (68) • From Address (73) • Host Name (70) • Object CUID (92) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Port (72) • Publication Instance ID (82) • Recipient Name (80) • Template Document CUID (91) • To Address (74) • User Groups (42) • User Name (69)

Event service auditing events

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
262145	Event registered	<ul style="list-style-type: none"> • Event filename (41) • Event ID (40)
262146	Event unregistered	<ul style="list-style-type: none"> • Event Filename (41) • Event ID (40)
262147	Event updated	<ul style="list-style-type: none"> • Event filename (41) • Event ID (40)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
262148	Event triggered	<ul style="list-style-type: none"> • Event filename (41) • Event ID (40)

Report Application service auditing events

The Report Application service (RAS) is used to create reports using custom applications developed with the RAS SDK. All of the following codes will be generated by custom applications. Consult your RAS SDK documentation for additional details.

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
458753	<p>Report was opened for viewing and/or modification</p> <p>Note: In a few cases, this Event_Type_ID may be generated when the report opens but cannot be viewed. This may occur when:</p> <ul style="list-style-type: none"> • There are problems with the database setup for the report. For example, you may see this message when the database driver for the report is not present on the client machine • A processing extension associated with the report aborts viewing, or fails. • The report used Business Views and the user did not have permissions to refresh the underlying data connections. • The machine running the RAS ran out of space in its temporary directory. 	<ul style="list-style-type: none"> • Object CUID (92) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Parent Document CUID (91) • User Groups (42)
458754	Report was saved to the CMS.	
458755	Report was created and saved to the CMS	
458756	Report could not be opened.	
458757	Report could not be saved to the CMS.	

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
458758	Report could not be created in the CMS.	

Web Intelligence and Desktop Intelligence auditing events

Note:

- The list of auditable events for Desktop Intelligence and Web Intelligence Rich Client only apply when the client is actively logged in to BusinessObjects Enterprise. If the client is being use in an offline mode then events will not be recorded.
- If a document is imported to the Web Intelligence Rich Client and worked on as a local document, all auditing events regarding that document will be reported as Web Intelligence client events and contain the details (name, CUID etc.) of the locally saved version of that document, not the repository version. Repository events will be reported by the Web Intelligence Processing Server, and client events will be reported by the Adaptive Processing Server with Client Auditing Proxy Service enabled.

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
6	List of Universes Retrieved	<ul style="list-style-type: none"> • Number of elements (7) • Session ID (45) • User Groups (42)
9	Document Saved	<ul style="list-style-type: none"> • Description (14) • Document name (8) • Document size (9) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Options Refreshed (17) • Overwrite (18) • Session ID (45) • User Groups (42)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
11	Document Retrieved	<ul style="list-style-type: none"> • Document name (8) • Document size (9) • Object CUID (92) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Parent Document CUID (91) • Session ID (45) • User Groups (42)
13	Universe Selected	<ul style="list-style-type: none"> • Session ID (45) • Universe Name (2) • User Groups (42)
19	Document refreshed Note: This event will also occur when a user creates a document	<ul style="list-style-type: none"> • Document Name (8) • Number of lines (6) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Parent Document CUID (91) • Session ID (45) • SQL value (19) • Universe name (2) • User Groups (42)
21	List of Values Retrieved	<ul style="list-style-type: none"> • Number of lines (6) • Object Name (3) • Session ID (45) • Universe name (2) • User Groups (42)
22	Document Edited	<ul style="list-style-type: none"> • Document name (8) • Session ID (45) • User Groups (42)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
28	Apply format	<ul style="list-style-type: none"> Document name (8) Report name (22) Session ID (45) User Groups (42)
40	Get page	<ul style="list-style-type: none"> Document name (8) Document type (21) Object CUID (92) Object Folder Path (43) Object instance (90) Object Name (3) Parent Document CUID (91) Session ID (45) User Groups (42)
41	SQL Generated	<ul style="list-style-type: none"> Document name (8) Object Folder Path (43) Object instance (90) Object Name (3) Parent Document CUID (91) Session ID (45) SQL value (19) Universe name (2) User Groups (42)
42	Drill out of scope	<ul style="list-style-type: none"> Document name (8) Number of lines (6) Object Folder Path (43) Object instance (90) Object Name (3) Session ID (45) SQL value (19) Universe name (2) User Groups (42)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
43	Prompt Selected	<ul style="list-style-type: none"> • Document name (8) • Object Folder Path (43) • Object instance (90) • Object Name (3) • Parent Document CUID (91) • Prompt Named • Prompt value • Session ID (45) • User Groups (42)
50	sendtousers	
51	startdesktopapp Note: Desktop Intelligence only.	<ul style="list-style-type: none"> • Object Folder Path (43) • Object Name (3) • User Groups (42)

Voyager auditing events

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
12500	MDAS Session Creation	<ul style="list-style-type: none"> • Object Folder Path (43) • Object Name (3) • User Groups (42)
12501	MDAS Session Closed	<ul style="list-style-type: none"> • Object Folder Path (43) • Object Name (3) • User Groups (42)
12502	MDAS Cube Connection Opened	<ul style="list-style-type: none"> • Object Folder Path (43) • Object Name (3) • User Groups (42)

Event_Type_ID	Event_Type_Description	Event Details (Detail_ID)
12503	MDAS Cube Connection Closed	<ul style="list-style-type: none"> Object Folder Path (43) Object Name (3) User Groups (42)
12504	MDAS Connection Failure	<ul style="list-style-type: none"> Object Folder Path (43) Object Name (3) User Groups (42)

Client events

Event_Type_ID	Event_Type_Description	Description
50	sendtousers	Triggered by a Desktop Intelligence application sending an object to a user.
51	startdesktopapp	Triggered by the startup of Desktop Intelligence.

Detail Codes reference table

Detail_ID	Detail_Description	Description
2	Universe name	
3	Object Name	
6	Number of lines	
7	Number of elements	
8	Document name	
9	Document size	
14	Description	

Detail_ID	Detail_Description	Description
15	Category name	
16	Keywords	
17	Options Refreshed	
18	Overwrite	
19	SQL value	
21	Document type	
22	Report name	
23	Prompt Named	
24	Prompt value	
30	Data Provider Name	
31	Page Range	
40	Event ID	
41	Event Filename	
42	User Groups	
43	Object Folder Path	
44	Object Category Path	
45	Session ID	
46	Enterprise Error Text	
47	ODBC SQLSTATE	
48	ODBC Error Text	
49	BOE UserID	

Detail_ID	Detail_Description	Description
50	Object Type	
51	Report Data Type	
60	IP address reported by client	Triggered during thick-client (CORBA) logon. Records the IP address reported by the client.
61	Hostname reported by client	Triggered during thick-client (CORBA) logon. Records the host machine name reported by the client.
62	IP address resolved by server	Triggered during thin and thick client logon. Records the IP address of the client as reported by the server. This is more reliable than "IP address reported by client", but servers may not be able to correctly resolve IP addresses on some networks.
63	Hostname resolved by server	Triggered during thin and thick client logon. Records the host machine name of the client as reported by the server. This is more reliable than "hostname reported by client", but servers may not be able to correctly resolve client host names on some networks.
64	Logon using token	
65	Destination Type	Indicates intended destination of job (printer, folder, email, etc.).
66	Destination Delivery Type	Indicates if job was a scheduled operation or user initiated.
67	Directory	Records the directory the object or instance is transferred to. Triggered only if a job is communicated using FTP.

Detail_ID	Detail_Description	Description
68	File Name	Records the file name of the object or instance. Triggered only if a job is communicated using FTP or email.
69	User Name	Records the name of the user who requested the event. Triggered only by user-initiated delivery of an object.
70	Host Name	Records the name of the host machine of the intended recipient of the object or instance. Triggered only if a job is published by email or FTP.
71	Domain	Records the email domain it is sent to. Triggered only if a job is published by email.
72	Port	Records the port used in the file transfer. Triggered only if a job is communicated using FTP or email.
73	From Address	Triggered only by email delivery of object.
74	To Address	Triggered only by email delivery of object.
75	CC Address	Triggered only by email delivery of object.
76	Error Message	Records any error messages generated by the failure of a job.
80	Recipient Name	Records the name of the intended recipient (if provided by the job).
81	Document Scope	
82	Publication Instance ID	Records a unique instance ID for that event.
89	Concurrent User Count	

Detail_ID	Detail_Description	Description
90	Object instance	
91	Parent Document CUID	
92	Object CUID	
93	Right added	
94	Right removed	
95	Right modified	
100	Number of Copies Printed	
12500	MDAS General Failure	
12501	MDAS Credential Failure	

Application_Type table reference

Application_Type_ID	Application_Type_Description
0	PM Rules Service
1	Dashboard Analytics Service
2	Client Auditing Proxy Service
3	Auditing Service
4	Scheduling Host Service
5	Crystal Reports Scheduling Service
6	Crystal Reports Cache Service

Application_Type_ID	Application_Type_Description
7	Central Management Service
8	Connection Service
9	Crystal Reports Viewing and Modification Service
10	Dashboard Service
11	Desktop Intelligence Scheduling Service
12	Desktop Intelligence Cache Service
13	Desktop Intelligence Processing Service
14	Destination Delivery Scheduling Service
15	Destination Configuration Service
16	PM Visualization Cache Service
17	PM Visualization Processing Service
18	Event Service
19	Sets Profiler Service
20	Input Filestore Service
21	Scheduling Host Service
22	List Of Values Scheduling Service
23	PM Metric Aggregation Service
24	Output Filestore Service
25	Crystal Reports Processing Service
26	Predictive Analytic Service

Application_Type_ID	Application_Type_Description
27	Program Scheduling Service
28	Publication Scheduling Service
29	Publishing Post Processing Service
30	Publishing Service
31	Replication Service
32	PM Repository Management Service
33	Single Sign-On Service
34	Sets Query Service
35	Process Analysis Service
36	Web Intelligence Scheduling and Publishing Service
37	Web Intelligence Processing Service
38	Desktop Intelligence
39	Search Service
40	Multi-Dimensional Analysis Service
41	Web Intelligence



Server Command Lines



14

chapter



This section lists the command-line options that control the behavior of each BusinessObjects Enterprise server.

Click the appropriate link to jump to that section:

- [Command lines overview](#)
- [Standard options for all servers](#)
- [Central Management Server](#)
- [Crystal Reports Processing Server and Crystal Reports Cache Server](#)
- [Job servers](#)
- [Report Application Server](#)
- [Input and Output File Repository Servers](#)
- [Event Server](#)
- [Web Intelligence Processing Server](#)

Command lines overview

When you start or configure a server through the Central Management Console (CMC) or the Central Configuration Manager (CCM), the server is started (or restarted) with a default command line that includes a typical set of options and values. In the majority of cases, you need not modify the default command lines directly. Moreover, you can manipulate the most common settings through the various server configuration screens in the CMC and the CCM. For reference, this section provides a full listing of the command-line options supported by each server. You can modify each server's command line directly if you need to further customize the behavior of BusinessObjects Enterprise.

Throughout this section, values provided in square brackets [] are optional.

To view or modify a server's command line

The procedure for viewing or modifying a server's command line depends upon your operating system:

1. On Windows, use the CCM to stop the server. Then open the server's Properties to modify the command line. Start the server again when you have finished.
2. On UNIX, run `ccm.sh` to stop the server. Then edit `ccm.config` to modify the server's command line. Start the server again when you have finished.

Note:

On UNIX, each server's command line is actually passed as an argument to the `crystalrestart.sh` script. This script launches the server and monitors it in case an automatic restart is required. For more information, see the UNIX Tools chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

Click the appropriate link to jump to that section:

- [Standard options for all servers](#)
- [Central Management Server](#)
- [Crystal Reports Processing Server and Crystal Reports Cache Server](#)
- [Job servers](#)
- [Report Application Server](#)
- [Input and Output File Repository Servers](#)
- [Event Server](#)

Standard options for all servers

These command-line options apply to all of the BusinessObjects Enterprise servers, unless otherwise indicated. See the remainder of this section for options specific to each type of server.

Option	Valid Arguments	Behavior
-name	<i>string</i>	<p>Specify the friendly name of the server. The server registers this name with the Central Management Server (CMS), and the name is displayed in the CMC. The default friendly name is <i>host name.servertype</i></p> <p>Note:</p> <ul style="list-style-type: none"> Do not modify -name for a CMS. If you modify -name for an Input or Output File Repository Server, you must include "Input." or "Output." as the prefix to the value you type for <i>string</i> (for example, -name Input.Server01 or -name Output.UK).

Option	Valid Arguments	Behavior
<code>-ns</code>	<code>cmsname[:port]</code>	In previous versions, this setting was used to specify the CMS that the server should register with. Note that you can no longer use the <code>-ns</code> option on the server command line to configure which CMS a server should register with. This is now handled automatically by the Server Intelligence Agent.
<code>-requestPort</code>	<code>port</code>	Specify the port that the server listens on. The server registers this port with the CMS. If unspecified, the server chooses any free port > 1024. Note: This port is used for different purposes by different servers. Before changing, see the section on changing the default server port numbers in the <i>SAP BusinessObjects Enterprise Administrator's Guide</i> .
<code>-restart</code>		Server restarts if it exits with an unusual exit code.

Option	Valid Arguments	Behavior
-fg		UNIX only. Run the daemon in the foreground. When passing the server's command line to the <code>crystal restart.sh</code> script, you must use this option (see <code>ccm.config</code>). If you run the server's command line directly, do not use this option, because the foreground process blocks the shell until the server exits.

UNIX signal handling

On UNIX, the BusinessObjects Enterprise daemons handle the following signals:

- `SIGTERM` results in a graceful server shutdown (exit code = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE`, and `SIGILL` result in a rapid shutdown (exit code = 1).

Central Management Server

This section provides the command-line options that are specific to the CMS. The default path to the server on Windows is:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\CMS.exe
```

The default path to the server on UNIX is:

```
INSTALL_ROOT/bobje/enterprise120/platform/boe_cmsd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
-threads	<i>number</i>	Specifies the number of working threads that the CMS initializes and uses. The value can be between 12 and 150, and is set to 50 by default.
-reinitializedb		Cause the CMS to delete the system database and recreate it with only the default system objects.
-quit		Force the CMS to quit after processing the <code>-reinitializedb</code> option.

Option	Valid Arguments	Behavior
<code>-receiverPool</code>	<i>number</i>	Specify the number of threads the CMS creates to receive client requests. A client may be another Business Objects server, the Report Publishing Wizard, Crystal Reports, or a custom client application that you have created. The default value is 5. Normally you will not need to increase this value, unless you create a custom application with many clients.
<code>-maxobjectsincache</code>	<i>number</i>	Specify the maximum number of objects that the CMS stores in its memory cache. Increasing the number of objects reduces the number of database calls required and greatly improves CMS performance. However, placing too many objects in memory may result in the CMS having too little memory remaining to process queries. The upper limit is 100000.

Option	Valid Arguments	Behavior
<code>-ndbqthreads</code>	<i>number</i>	Specify the number of CMS worker threads sending requests to the database. Each thread has a connection to the database, so you must be careful not to exceed your database capacity. In most cases, the maximum value you should set is 10.
<code>-oobthreads</code>	<i>number</i>	If your cluster includes more than eight CMS cluster members, ensure that the command-line for each CMS includes this option. Specify the number of CMS services in your cluster. This option ensures that the cluster can sustain heavy load.
<code>-AuditInterval</code>	<i>minutes</i>	Specify interval at which the CMS requests audit information from audited servers. The default value is 5 minutes. (Maximum value is 15 minutes, and minimum value is 1 minute.).

Option	Valid Arguments	Behavior
<code>-AuditBatchSize</code>	<i>number</i>	Specify the maximum number of audit records that the CMS requests from each audited server, per audit interval. The default value is 200 records. (Maximum value is 500, and minimum value is 50.)
<code>-auditMaxEventsPerFile</code>	<i>number</i>	Specify the maximum number of records in the audit log file. The default value is 500. If the number specified by <code>-auditMaxEventsPerFile</code> is exceeded, the server opens a new log file.

Option	Valid Arguments	Behavior
<code>-AuditeeTimeSyncInterval</code>	<i>minutes</i>	Specify the interval between time synchronization events. The CMS broadcasts its system time to audited servers at the interval specified by <code>-AuditeeTimeSyncInterval</code> . The audited servers compare their internal clocks to the CMS time, and then adjust the timestamps they give to all subsequent audit records so that the time of these records synchronizes with the CMS time. The default interval is 60 minutes. (Maximum value is 1 day, or 1440 minutes. Minimum value is 15 minutes. Setting the interval to 0 turns off time synchronization.)

Central Configuration Manager (CCM)

You can now use the command line to perform tasks in the CCM on Windows. The default path on Windows is:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\ccm.exe
```

For a complete list of the commands available for the `ccm.exe`, run `ccm.exe -help`, or see the table in [ccm.sh](#).

For a list of standard command-line options, see [Standard options for all servers](#).

Crystal Reports Processing Server and Crystal Reports Cache Server

The Crystal Reports Processing Server and the Crystal Reports Cache Server are controlled in much the same way from the command line. The command-line options determine whether the server starts as a Processing Server, a Cache Server, or both. Options that apply only to one server type are noted below.

The default paths to the servers on Windows are:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\cacheserver.exe
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\pageserver.exe
```

The default paths to the servers on UNIX are:

```
INSTALL_ROOT/bobje/enterprise120/platform/boe_cachesd
INSTALL_ROOT/bobje/enterprise120/platform/boe_pagesd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
-cache		Enable Cache Server functionality.

Option	Valid Arguments	Behavior
<code>-dir</code>	<i>absolutePath</i>	Specify the cache directory for a Cache Server and the temp directory for the Processing Server. The directories created are <code>absolutePath/cache</code> and <code>absolutePath/temp</code> .
<code>-deleteCache</code>		Delete the cache directory every time the server starts and stops.
<code>-psdir</code>	<i>absolutePath</i>	Specify the temp directory for the Processing Server. This option overrides <code>-dir</code> .
<code>-refresh</code>	<i>minutes</i>	Share cached pages for the specified number of minutes.

Option	Valid Arguments	Behavior
<code>-maxDBResultRecords</code>	<i>number</i>	Limit the number of database records that are returned from the database. The default limit is 20000 records. If a user views an on-demand report containing more than 20000 records, an error message indicates that the report contains too many database records. To increase the enforced limit, increase <i>number</i> accordingly; to disable the limit, replace <i>number</i> with 0 (zero).
<code>-noautomaticdbdisconnect</code>		Disable automatic database disconnection for the Processing Server. By default the Processing Server will automatically disconnect from the reporting database after retrieving data, to free up database licenses. This may affect performance if your site uses many reports with on-demand subreports, or group-by-on-server.

Option	Valid Arguments	Behavior
<code>-report_ProcessExtPath</code>	<i>absolute path</i>	Specify the default directory for processing extensions. For details, see the <i>SAP BusinessObjects Enterprise Administrator's Guide</i> .
<code>-auditMaxEventsPerFile</code>	<i>number</i>	On the Cache Server, specifies the maximum number of audit actions recorded in the audit log file. The default value is 500. If this maximum number of records is exceeded, the server will open a new log file.

Job servers

This section provides the command-line options that are specific to the job servers, which include Job Servers, Program Job Servers, Destination Job Server, and List of Values Job Server.

The default path to the server on Windows is:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe
```

The default paths to the server on UNIX are:

```
INSTALL_ROOT/bobje/enterprisell/platform/boe_reportjobsd
INSTALL_ROOT/bobje/enterprisell/platform/boe_programjobsd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
-dir	<i>absolute path</i>	Specify the data directory for the Job Server.
-lib	<i>processing library</i>	<p>Specify the processing library to load:</p> <ul style="list-style-type: none"> • <code>procReport</code> or • <code>procProgram</code> <p>Loading <code>procReport</code> starts the Job Server as a Report Job Server. Loading <code>procProgram</code> starts the Job Server as a Program Job Server. This option is used in conjunction with <code>-objectType</code>.</p>

Option	Valid Arguments	Behavior
<code>-objectType</code>	<i>progID</i>	<p>The program ID of the processing library, which determines the class of object supported by the Job Server:</p> <ul style="list-style-type: none"> • <code>CrystalEnterprise.Report</code> or • <code>CrystalEnterprise.Program</code> <p>Used with <code>-lib</code> to specify whether the Job Server becomes a Report Job Server or a Program Job Server.</p>
<code>-maxJobs</code>	<i>number</i>	Set the maximum number of concurrent jobs that the server will handle. The default is five.
<code>-requestJSChildPorts</code>	<i>lowerbound-upper bound</i>	<p>Specify the range of ports that child processes should use in a firewall environment. For example, <code>6800-6805</code> limits child processes to six ports.</p> <p>Note: For this option to take effect, you must also specify the <code>-requestPort</code> setting.</p>

Option	Valid Arguments	Behavior
<code>-report_ProcessExtPath</code>	<i>absolute path</i>	Specify the default directory for processing extensions. For details, see the <i>SAP BusinessObjects Enterprise Administrator's Guide</i> .
<code>-auditMaxEventsPerFile</code>	<i>number</i>	Specify the maximum number of records in the audit log file. The default value is 500. If the number specified by <code>-auditMaxEventsPerFile</code> is exceeded, the server opens a new log file.

Report Application Server

This section provides the command-line options that are specific to the Report Application Server.

The default path to the server on Windows is:

```
C:\Program Files\Common Files\Business Objects\3.0\
bin\crystalras.exe
```

The default path to the server on UNIX is:

```
INSTALL_ROOT/bobje/enterprise120/platform/ras/boe_crystalrasd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
<code>-ipport</code>	<i>port</i>	Specify the port number for receiving TCP/IP requests when running in stand-alone mode (outside of BusinessObjects Enterprise).
<code>-report_ProcessExtPath</code>	<i>absolutepath</i>	Specify the default directory for processing extensions. For details, see the <i>SAP BusinessObjects Enterprise Administrator's Guide</i> .

Option	Valid Arguments	Behavior
<code>-ProcessAffinityMask</code>	<i>mask</i>	

Option	Valid Arguments	Behavior
		<p>Use a mask to specify exactly which CPUs that RAS will use when it runs on a multi-processor machine.</p> <p>The mask is in the format <code>0xffffffff</code>, where each <code>f</code> represents a processor, and the list of processors reads from right to left (that is, the last <code>f</code> represents the first processor). For each <code>f</code>, substitute either 0 (use of CPU not permitted) or 1 (use of CPU is permitted).</p> <p>For example, if you run the RAS on a 4 processor machine and want it to use the 3rd and 4th processor, use the mask <code>0x1100</code>. To use the 2nd and 3rd processor, use <code>0x0110</code>.</p> <p>Note:</p> <ul style="list-style-type: none"> RAS uses the first permitted processors in the string, up to the maximum specified by your license. If you have a two processor license, <code>0x1110</code> has the same effect as

Option	Valid Arguments	Behavior
		0x0110. <ul style="list-style-type: none"> The default value of the mask is -1, which has the same meaning as 0x1111.
-auditMaxEventsPerFile	<i>number</i>	Specify the maximum number of records in the audit log file. The default value is 500. If the number specified by -auditMaxEventsPerFile is exceeded, the server opens a new log file.

Web Intelligence Processing Server

This section provides the command-line options that are specific to the Web Intelligence Processing Server.

The default path to the server on Windows is:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\WIProcessingServer.exe
```

The default path to the server on UNIX is:

```
INSTALL_ROOT/bobje/enterprise120/platform/ras/boe_crystalrasd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
-ConnectionTimeout Minutes	<i>minutes</i>	Specify the number of minutes before the server will timeout.
-MaxConnections	<i>number</i>	Specify the maximum number of simultaneous connections that the server allows at one time.
-DocExpressEnable		Enables caching of Web Intelligence documents when the document is being viewed.
-DocExpressReal Time CachingEnable		Enables real time caching of Web Intelligence documents.
-DocExpressCache DurationMinutes	<i>minutes</i>	Specify the amount of time (in minutes) that content is stored in cache.
-DocExpressMax Cache SizeKB	<i>kilobytes</i>	Specify the size of the document cache.

Option	Valid Arguments	Behavior
-EnableListOfValuesCache		Enables the caching per user sessions of lists of values
-ListOfValuesBatchSize	<i>number</i>	Specify the maximum number of values that can be returned per list of values batch.
-UniverseMaxCacheSize	<i>number</i>	Specify the number of universes to be cached.
-WIDMaxCacheSize	<i>number</i>	Specify the maximum number of Web Intelligence documents that can be stored in cache.

Input and Output File Repository Servers

This section provides the command-line options that are specific to the Input and Output File Repository Servers.

The default paths to the servers on Windows are:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\inputfilesrv.exe
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\outputfilesrv.exe
```

The default paths to the program that provides both servers on UNIX are:

```
INSTALL_ROOT/bobje/enterprise120/platform/boe_inputfilesd
INSTALL_ROOT/bobje/enterprise120/platform/boe_outputfilesd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
<code>-rootDir</code>	<i>absolutepath</i>	<p>Set the root directory for the various subfolders and files that are managed by the server. File paths used to refer to files in the File Repository Server are interpreted relative to this root directory.</p> <p>Note: All Input File Repository Servers must share the same root directory, and all Output File Repository Servers must share the same root directory (otherwise there is a risk of having inconsistent instances). Additionally, the input root directory must not be the same as the output root directory. It is recommended that you replicate the root directories using a RAID array or an alternative hardware solution.</p>

Option	Valid Arguments	Behavior
<code>-tempDir</code>	<i>absolutePath</i>	<p>Set the location of the temporary directory that the FRS uses to transfer files. Use this command line option if you want to control the location of the FRS temporary directory, or if the default temporary directory name generated by the FRS exceeds the file system path limit (which will prevent the FRS from starting).</p> <p>Note: Do not specify an existing directory for this option. The specified directory will be emptied when the FRS starts, and removed when the FRS shuts down. If you use an existing directory, it will be emptied and removed.</p>
<code>-maxidle</code>	<i>minutes</i>	Specify the number of minutes after which an idle session is cleaned up.

Event Server

This section provides the command-line options that are specific to the Event Server.

The default path to the server on Windows is:

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\EventServer.exe
```

The default path to the server on UNIX is:

```
INSTALL_ROOT/bobje/enterprise120/platform/boe_eventsd
```

For a list of standard command-line options, see [Standard options for all servers](#).

Option	Valid Arguments	Behavior
-poll	<i>seconds</i>	Specify the frequency (in seconds) with which the server checks for File events.
-cleanup	<i>minutes</i>	Specify the frequency (in minutes) with which the server cleans up listener proxies. The value represents the amount of time it takes to perform two cleanups. For example, if you specify a value of 10, the proxies will be cleaned up every 5 minutes.

Option	Valid Arguments	Behavior
<code>-auditMaxEventsPerFile</code>	<i>number</i>	Specify the maximum number of records in the audit log file. The default value is 500. If the number specified by <code>-auditMaxEventsPerFile</code> is exceeded, the server opens a new log file.



UNIX Tools

15

chapter



This section details each of the administrative tools and scripts that are included with the UNIX distribution of BusinessObjects Enterprise. This section is provided primarily for reference purposes. Concepts and configuration procedures are discussed in more detail throughout this guide.

Script utilities

This section describes the administrative scripts that assist you in working with BusinessObjects Enterprise on UNIX. The remainder of this help discusses the concepts behind each of the tasks that you can perform with these scripts. This reference section provides you the main command-line options and their arguments.

ccm.sh

The `ccm.sh` script is installed to the `boobje` directory of your installation. This script provides you with a command-line version of the CCM. This section lists the command-line options and provides some examples.

Note:

- Arguments in square brackets [] are optional.
- If you are unsure of a Server Intelligence Agent's fully qualified name, look at the Command properties in the `ccm.config` file, and use the value that appears after the `-nodename` option.
- Arguments denoted by *other authentication information* are provided in the second table.

CCM Option	Valid Arguments	Description
<code>-help</code>	n/a	Display command-line help.

CCM Option	Valid Arguments	Description
-start	all or <i>sianame</i>	Start each Server Intelligence Agent as a process. Use the short form of the SIA name.
-stop	all or <i>sianame</i>	Stop each Server Intelligence Agent by terminating its Process ID. Use the short form of the SIA name.
-restart	all or <i>sianame</i>	Stop each Server Intelligence Agent by terminating its Process ID; then each SIA is started. Use the short form of the SIA name.
-managedstart	<fully qualified server name>[other authentication information]	Start a server as a process.
-managedstop	<fully qualified server name>[other authentication information]	Stop a server by terminating its Process ID.
-managedrestart	<fully qualified server name>[other authentication information]	Stop a server by terminating its Process ID; then start the server.

CCM Option	Valid Arguments	Description
-managedforceterminate	<i><fully qualified server name>[other authentication information]</i>	Stops the server immediately without completing current processing requests.
-enable	<i><fully qualified server name>[other authentication information]</i>	Enable a started server so that it registers with the system and starts listening on the appropriate port. Use the fully qualified form of the server name.
-disable	<i><fully qualified server name>[other authentication information]</i>	Disable a server so that it stops responding to BusinessObjects Enterprise requests but remains started as a process. Use the fully qualified form of the server name.

CCM Option	Valid Arguments	Description
<code>-display</code>	<i>[other authentication information]</i>	Reports the server's current status (enabled or disabled). The CMS must be running before you can use this option.
<code>-updateobjects</code>	<i>[other authentication information]</i>	Update objects migrated from a previous version of BusinessObjects Enterprise into your current CMS system database. Use this option after running <code>cmsdbsetup.sh</code> .

The following table describes the options that make up the argument denoted by *[other authentication information]*.

Authentication Option	Valid arguments	Description
<code>-cms</code>	<i>cmsname:port#</i>	Specify the CMS that you want to log on to. If not specified, the CCM defaults to the local machine and the default port (6400).

Authentication Option	Valid arguments	Description
<code>-username</code>	<i>username</i>	Specify an account that provides administrative rights to BusinessObjects Enterprise. If not specified, the default Administrator account is attempted.
<code>-password</code>	<i>password</i>	Specify the corresponding password. If not specified, a blank password is attempted. Note: To specify the <code>-password</code> argument, you must also specify the <code>-username</code> argument.
<code>-authentication</code>	<code>secEnterprise</code> , <code>se</code> <code>cLDAP</code>	Specify the appropriate authentication type for the administrative account. If not specified, <code>secEnterprise</code> is attempted.

The CCM reads the launch strings and other configuration values from the `ccm.config` file. For details, see [ccm.config](#).

Examples

These two commands start and enable all Server Intelligence Agents. The Central Management Server (CMS) is started on the local machine and the default port (6400):

```
ccm.sh -start all  
ccm.sh -enable all
```

These two commands start and enable all the Server Intelligence Agents. The CMS is started on port 6701, rather than on the default port:

```
ccm.sh -start all  
ccm.sh -enable all -cms MACHINE01:6701
```

These two commands start and enable all the Server Intelligence Agents with a specified administrative account named SysAdmin:

```
ccm.sh -start all  
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin  
-password 35%bC5@5 -authentication LDAP
```

This single command logs on with a specified administrative account to disable a Job Server that is running on a second machine:

```
ccm.sh -disable MACHINE02.businessobjects.com.reportserver  
-cms MACHINE01:6701 -username SysAdmin -password  
35%bC5@5 -authentication secLDAP
```

ccm.config

This configuration file defines the launch strings and other values that are used by the CCM when you run its commands. This file is maintained by the CCM itself, and by the other BusinessObjects Enterprise script utilities. You typically edit this file only when you need to modify a Server Intelligence Agent's command line. For details, see [Command lines overview](#).

cmsdbsetup.sh

The `cmsdbsetup.sh` script is installed to the `bobje` directory of your installation. The script provides a text-based program that enables you to configure the CMS database, CMS clusters, and to set up the audit database.

You can add a CMS to a cluster by selecting a new data source for its CMS database. You can also delete and recreate (re-initialize) a CMS database, copy data from another data source, or change the existing cluster name.

Note:

Before running this script, back up your current CMS database. Also be sure to see [Clustering Central Management Servers](#) for additional information about CMS clusters and configuring the CMS database.

The script will prompt you for the name of your Server Intelligence Agent (SIA). To check the name of your SIA, view the Command properties of the SIA. The SIA's current name appears after the `-nodename` option.

For more information about configuring the CMS database or setting up the auditing database, see [Managing Auditing](#).

configpatch.sh

The `configpatch.sh` script is installed to the `bobje/enterprise/generic` directory of your installation. Use the `configpatch.sh` script when installing patches that require updates to system configuration values. After installing the patch, run `configpatch.sh` with the appropriate `.cf` file name as an argument. The `readme.txt` file that accompanies BusinessObjects Enterprise patches tells you when to run `configpatch.sh`, and the name of the `.cf` file to use.

serverconfig.sh

The `serverconfig.sh` script is installed to the `bobje` directory of your installation. This script provides a text-based program that enables you to view server information and to add and delete servers from your installation.

This script adds, deletes, modifies, and lists information from the `ccm.config` file.

When you modify a server using `serverconfig.sh`, you can change the location of its temporary files. For the Central Management Server, you can change its port number or enable auditing. For the Input File Repository Server or the Output File Repository Server, you can enter the root directory.

To add/delete/modify/list UNIX servers

1. Go to the `bobje` directory of your installation.
2. Issue the following command:

```
./serverconfig.sh
```

The script prompts you with a list of options:

- 1 - Add a Server Intelligence Agent
 - 2 - Delete a Server Intelligence Agent
 - 3 - Modify a Server Intelligence Agent
 - 4 - List all Server Intelligence Agent in the config file
3. Type the number that corresponds to the action you want to perform.
 4. If you are adding, deleting, or modifying a server, provide the script with any additional information that it requests.

Tip:

The script will prompt you for the name of your CMS. By default, the CMS name is `hostname.cms`. That is, the default name of a CMS installed on a machine called `MACHINE01` is `MACHINE01.cms`. However, in this script you can enter `hostname` to check the name of your CMS (or any other server), view the contents of `ccm.config`, and look for the server's launch string. The server's current name appears after the `-name` option.

5. Once you have added or modified a server, use the CCM to ensure that the server is both started and enabled.

For more information about working with servers, see [Server management overview](#).

uninstallBOBJE.sh

The `uninstallBOBJE.sh` script is installed to the `bobje` directory of your installation. This script deletes all of the files installed during your original installation of BusinessObjects Enterprise by running the scripts in the `bobje/uninstall` directory. Do not run the scripts in the `uninstall` directory yourself: each of these scripts removes only the files associated with a single BusinessObjects Enterprise component, which may leave your BusinessObjects Enterprise system in an indeterminate state.

Before running this script, you must disable and stop all of the BusinessObjects Enterprise servers.

Note:

- The `uninstallBOBJE.sh` script will not remove files created during the installation process, or files created by the system or by users after installation. To remove these files, after running `installBOBJE.sh`, perform an `rm -rf` command on the `bobje` directory.
- If you performed the "system" installation type, you will also need to delete the run control scripts from the appropriate `/etc/rc#` directories.

Script templates

These scripts are provided primarily as templates upon which you can base your own automation scripts.

startservers

The `startservers` script is installed to the `bobje` directory of your installation. This script can be used as a template for your own scripts: it is provided as an example to show how you could set up your own script that starts the BusinessObjects Enterprise servers by running a series of CCM commands. For details on writing CCM commands for your servers, see [ccm.sh](#).

stopservers

The `stopservers` script is installed to the `bobje` directory of your installation. This script can be used as a template for your own scripts: it is provided as an example to show how you could set up your own script that stops the BusinessObjects Enterprise servers by running a series of CCM commands. For details on writing CCM commands for your servers, see [ccm.sh](#).

silentinstall.sh

The `silentinstall.sh` script is installed to the `bobje` directory of your installation. Once you have set up BusinessObjects Enterprise on one machine, you can use this template to create your own scripts that install BusinessObjects Enterprise automatically on other machines. Essentially, once you have edited the `silentinstall.sh` template accordingly, it defines the required environment variables, runs the installation and setup scripts, and sets up BusinessObjects Enterprise according to your specifications, without requiring any further input.

The silent installation is particularly useful when you need to perform multiple installations and do not want to interrupt people who are currently working on machines in your system. You can also use the silent installation script in your own scripts. For example, if your organization uses scripts to install software on machines, you can add the silent BusinessObjects Enterprise installation command to your scripts.

For information about script parameters, see the comments in the `silentinstall.sh` script.

Note:

- Because the `silentinstall.sh` file is installed with BusinessObjects Enterprise, you cannot install silently the first time you install BusinessObjects Enterprise.
- The silent installation is not recommended if you need to perform custom installations. The installation options are simplified and do not allow for the same level of customization provided in the BusinessObjects Enterprise install script.

Scripts used by BusinessObjects Enterprise

These secondary scripts are often run in the background when you run the main BusinessObjects Enterprise script utilities. You need not run these scripts yourself.

bobjerestart.sh

This script is run internally by the CCM when it starts the BusinessObjects Enterprise server components. If a server process ends abruptly without returning its normal exit code, this script automatically restarts a new server process in its place. Do not run this script yourself.

env.sh

The `env.sh` script is installed to the `bobje` directory of your installation. This script sets up the BusinessObjects Enterprise environment variables that are required by some of the other scripts. BusinessObjects Enterprise scripts run `env.sh` as required. When you install BusinessObjects Enterprise on UNIX, you must configure your Java application server to source this script on startup. See the *SAP BusinessObjects Enterprise Installation Guide* for more details.

env-locale.sh

The `env-locale.sh` script is used for converting the script language strings between different types of encoding (for example, UTF8 or EUC or Shift-JIS). This script is run by `env.sh` as needed.

initlaunch.sh

The `initlaunch.sh` script runs `env.sh` to set up the BusinessObjects Enterprise environment variables, and then runs any command that you have added as a command-line argument for the script. This script is intended primarily for use as a debugging tool by Business Objects SA.

patchlevel.sh

The `patchlevel.sh` is installed to the `bobje/enterprise/generic` directory of your installation. This script reports on the patch level of your UNIX distribution. This script is intended primarily for use by Business Objects SA support staff.

Option	Valid Arguments	Description
<code>list</code>	<code>n/a</code>	List all the installed patches.
<code>query</code>	<code>patch #</code>	Query the operating system for the presence of a particular patch by numeric ID.
<code>check</code>	<code>textfile</code>	Check that all the patches listed in <code>textfile</code> are installed on your operating system.

postinstall.sh

The `postinstall.sh` script is installed to the `bobje` directory of your installation. This script runs automatically at the end of the installation script and launches the `setup.sh` script. You need not run this script yourself.

setup.sh

The `setup.sh` script is installed to the `bobje` directory of your installation. This script provides a text-based program that allows you to set up your BusinessObjects Enterprise installation. This script is run automatically when you install BusinessObjects Enterprise. It prompts you for the information that is required in order to set up BusinessObjects Enterprise for the first time.

For complete details on responding to the setup script when you install BusinessObjects Enterprise, see the *SAP BusinessObjects Enterprise Installation Guide*.

setupinit.sh

The `setupinit.sh` script is installed to the `bobje` directory of your installation when you perform a system installation. This script copies the run control scripts to your `rc#` directories for automated startup. When you run a system installation you are directed to run this script after the `setup.sh` script completes.

Note:

You must have root privileges to run this script.



BIAR Command Line Tool

16

chapter



Biar Command Line Tool

The BIAR Engine Command Line Tool helps administrators and delegated administrators to promote content between Development, Quality Assurance, and Production BusinessObjects Enterprise XI 3.0 environments. The tool gives you the ability to use scripting to automate the import and export of objects.

The BIAR Command Line Tool only supports migrating objects from one XI 3.x system to another. You cannot use the tool to import objects from BusinessObjects, Crystal Enterprise, or earlier version of BusinessObjects Enterprise. You must use the Import Wizard to import content from previous versions of BusinessObjects to XI 3.x.

The Biar Engine Command Line tool is called `biarengine.jar`. On a windows environment, this file is located at *Install Directory\Business Objects\common\4.0\java\lib*. On UNIX, the file is located at *Install Directory/bobje/java/lib/*.

`InstallEntSdkWrapper.jar`, the command-line tool for importing BIAR files in BusinessObjects Enterprise XI Release 2, is not supported with BusinessObjects Enterprise XI 3.x. You must use `biarengine.jar` when importing content from BIAR files in BusinessObjects Enterprise XI 3.x.

Note:

- You must have a Java Runtime Environment installed. For supported a list of supported JREs, please see the BusinessObjects Enterprise supported platform document guide online on our support web site: http://support.businessobjects.com/documentation/supported_platforms.
- To use the BIAR Command Line Tool, you must have the Administrator account credentials for the XI 3.x environment that you are importing content to or from. You can also use a Delegated administrator account. For more information on using delegated administration to import content, see the *SAP BusinessObjects Enterprise XI 3.x Import Wizard Guide*.

The BIAR Command Line Tool imports the following types of objects:

Agnostic Documents	PDFs
Analytic Objects	PowerPoint Presentations
BI Modeler Objects	Profiles
Business Views	Programs
Calendars	Prompt Groups
Categories	Publications
Client Actions	Query as a Webservice
Custom Roles	Reports
Dashboards	Report Instances
Desktop Intelligence Documents	Rich Text Format Documents
Discussions	Server Groups
Encyclopedias	Shortcuts
Enterprise Users	Text Files
Events	Universes
Excel Spreadsheets	User Groups
Flash Files	Voyager Connections
Folders	Voyager Workspaces
FullClientAddins	Web Intelligence Documents
FullClientTemplates	WinAD Users
Hyperlinks	WinNT Users
LDAP Users	Word Documents
LOVs	Xcelcius Documents
Object Packages	XcelciusDMTTemplates
Overloads	

Importing relationships

The BIAR Command Line Tool only keeps the relationships between imported objects intact if both objects are imported together, or if one of the objects already exists on the destination. For example, if you have a Web Intelligence Report that uses a Universe, and you import the Report without also importing the Universe, the relationship between the two is dropped. The Report will not run on the destination.

Importing users and groups

If you are importing groups and users into a XI 3.0 environment, and a group already exists on the destination, the group membership on the destination is overwritten with the group membership that was exported from the *biar* file. This means if the group on the destination has additional users that are not contained in the group in the BIAR file group, they will not be part of the group after the import occurs.

Importing rights

The BIAR Engine Command Line Tool only imports rights on an object if the user/group is either exported with the object or already exists on the destination.

If the user/group and object already exist on the destination, the Tool overwrites the rights set on the object for this user/group on the destination with the imported rights.

However, if an object already exists on the destination and a user/group has rights specified on that object on the destination, but no rights for this user/group are specified on the object in the BIAR file, the Tool does not remove the existing rights for the user/group.

This means that rights that exist on a destination object can be overwritten, but never removed.

Using Multiple BIAR files

When using the BIAR Engine Command Line Tool to export content, the content is placed in a BIAR file. The location and name of the BIAR file is determined by *exportBiarLocation* parameter. When you export content that exceeds the amount of information that can be stored in a single BIAR file, the Tool splits the information and stores it in multiple BIAR files. The

files use the name that you specify, and will have numbers added to the end of the file name.

For example, if you set `exportBiarLocation= C:\Archive.biar`, and you export more content than can fit in a single BIAR file, the Tool creates the files `Archive.biar`, `Archive1.biar`, `Archive2.biar`, and so on. The Tool creates the files in the directory `C: .`

Note:

If you want to import content that is stored in multiple BIAR files, you must ensure that all of the BIAR files are located in the same directory.

The Biar Engine Command Line Tool's Properties File

The Biar Engine Command Line Tool requires a properties file that contains the parameters that tell the BIAR Engine what actions to take, what BusinessObjects Enterprise system to connect to and so on.

The file must have a `.properties` file extension. For example: `Myproperties.properties`

Parameter	Allowed Values	Description	Example
<code>Action</code>	<code>exportXML</code> , <code>importXML</code>	Specifies whether the Tool imports content from a BIAR file to a BusinessObjects Enterprise system, or exports the content from a deployment to a BIAR file. Mandatory.	<code>Action=exportXML</code>

Parameter	Allowed Values	Description	Example
<i>exportBiarLocation</i>	Free form text. Must include a .biar extension.	Specifies where the Tool saves the exported BIAR file. Mandatory if action=exportXML.	exportBiarLocation=C:/BiarExportFile.biar
<i>importBiarLocation</i>	Free form text. Must include a .biar extension.	Specifies where the BIAR file that is to be import is located. BIAR files are split if the contents are too large to fit into one BIAR file. You can enter any of the BIAR file partitions, but you must ensure all of the partitions are in the same directory Mandatory if action=importXML.	importBiarLocation=C:/BiarImportFile.biar
<i>userName</i>	Free form text.	The username of the an administrative account that the tool should use to connect to the Central Management Server (CMS). This can be the username of a Delegated Administrator account. Mandatory.	userName=Administrator

Parameter	Allowed Values	Description	Example
<i>password</i>	Free form text.	The password for the administrative account . Mandatory.	password=password
<i>authentication</i>	secEnterprise, secWinAd, secLdap	The authentication type that Tool uses. Optional. If you don't specify an authentication type, the default is secEnterprise.	authentication=secEnterprise
<i>CMS</i>	Free form text.	The name of the CMS that you want to connect to. Mandatory.	CMS=mycms:6400

Parameter	Allowed Values	Description	Example
<i>exportDependencies</i>	True, False	<p>Specifies whether to import all dependencies of an object. This should be used with care as it imports all the objects that are associated with any selected objects. This can increase the size of a BIAR file quite dramatically.</p> <p>Optional. If you don't specify a value, the default is False.</p> <p>Only used if action=exportXML.</p>	exportDependencies=false

Parameter	Allowed Values	Description	Example
<code>includeSecurity</code>	True, False	<p>Specifies whether the Tool exports and imports security associated with the objects and users that you select. If you want to maintain security it is important to set <i>includeSecurity</i> to true when exporting and importing content.</p> <p>Note: If you are using Access Levels, you must explicitly export these objects.</p> <p>Optional. If you don't specify a value for this parameter, the default is True.</p>	<code>includeSecurity=false</code>

Parameter	Allowed Values	Description	Example
<i>exportQuery</i>	Free form text, must use the CMS query language format.	<p>The queries the Tool should execute to gather the desired objects for exportation.</p> <p>You can use as many queries as you like in a single properties file, but the queries must be named “export-Query1”, “export-Query2”, and so on.</p> <p>Mandatory if action=exportXML.</p>	<pre>exportQuery=select * from ci_Infoobjects where si_name = 'Xtreme Employees' and si_kind = 'Webi'</pre>
<i>exportQueriesTotal</i>	Positive whole numbers.	<p>Specifies how many export queries the tool executes. If you have x export queries and want to execute them all, you must set this parameter to x.</p> <p>Optional. If you don't provide a value for this parameter, the default value is 1.</p> <p>Only used if action=exportXML.</p>	<pre>exportQueriesTo tal=5</pre>

Note:

To comment lines out, use the # character. For example:

```
action=importXML
#exportLocation=C:/mybiar.biar
importLocation=C:/mybiar.biar
```

This is an example of a properties file that imports content from a BIAR file.

```
#This file imports a biar, note this line is a comment
importBiarLocation=C:/CR.biar
action=importXML
userName=Administrator
password=
CMS=vanmsung01:6400
authentication=secEnterprise
```

This is an example of a properties file that exports a WebIntelligence report named “Xtreme Employees” to a BIAR file:

```
#This file exports a single report
# Remember to include indexed properties with your
query!
# The more indexed properties, the better!
exportBiarLocation=C:/CR.biar
action=importXML
userName=Administrator
password=
CMS=vanmsung01:6400
authentication=secEnterprise
exportDependencies=false
exportQuery= select * from ci_Infoobjects where si_name
= 'Xtreme Employees' and si_kind = 'Webi'
```

To use the BIAR Command Line Tool

1. Open a command line window.
2. In the command line window, navigate to the directory where the tool is located.

For example, *Install Directory\Business Objects\common\4.0\java\lib.*

3. Execute the biarengine.jar.

For example, `java -jar biarengine.jar <properties file>`

The BIAR Engine Command Line Tool either exports content from BusinessObjects Enterprise deployment to a BIAR file, or imports the content from a BIAR file to a BusinessObjects Enterprise deployment, depending on the action parameter in the properties file.



Working with the Central Management Console



17

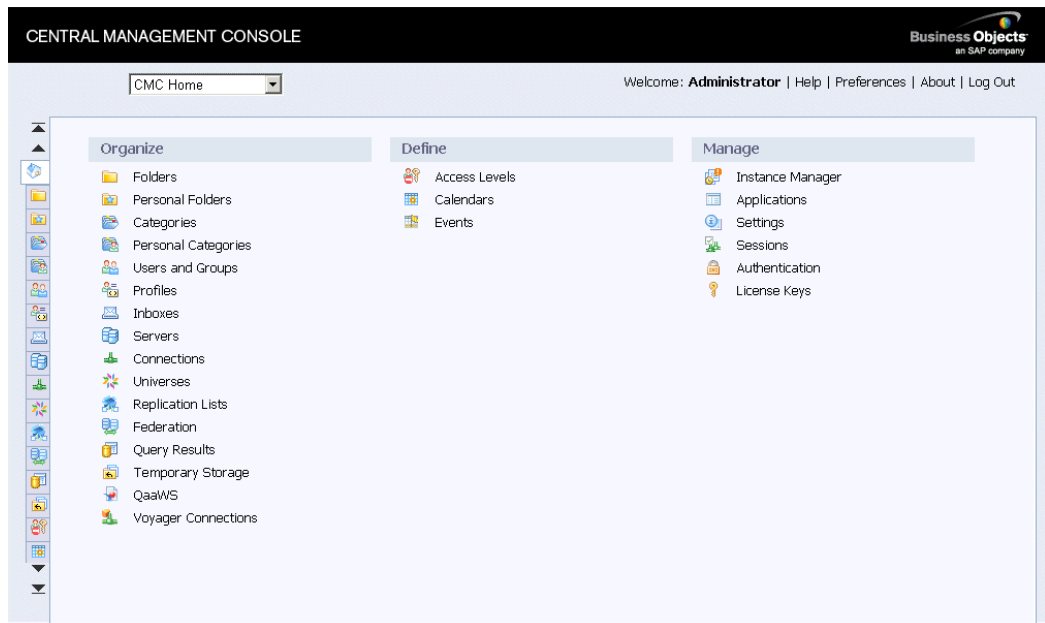
chapter

Overview

This section provides a general description of system administration as it relates to BusinessObjects Enterprise. It then introduces the administration tools that allow you to manage and configure BusinessObjects Enterprise, and it shows how to make some common changes to the system's default security settings.

Using the CMC

The Central Management Console (CMC) is a web-based tool which offers a single interface through which you can perform almost every day-to-day administrative task, including user management, content management, and server management.



Any user with valid credentials to BusinessObjects Enterprise can log on to the CMC and set his or her preferences. However, users who are not members of the Administrators group cannot perform any of the available management tasks unless they have been granted rights to do so.

Related Topics

- *How rights work in BusinessObjects Enterprise*

Logging on to the CMC

There are two ways to access the CMC: type the name of the machine you are accessing directly into your browser, or select **BusinessObjects Enterprise Central Management Console** from the program group on the Windows Start menu.

When you have finished using the CMC, end the session by logging off. The **Log Out** button is located in the upper-right corner of the console.

To log on to the CMC from your browser

1. Type the appropriate URL:
 - Go to the following page: `http://webserver:8080/CmcApp/`

Replace *webserver* with the name of the web server machine. If you changed this default virtual directory on the web server, you will need to type your URL accordingly. If necessary, change the default port number to the number you provided when you installed BusinessObjects Enterprise.

Tip:

On Windows, you can click **Start > Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > BusinessObjects Enterprise Central Management Console**.

If your CMC is hosted on a Web Application Container Server (WACS), you can click **Start > Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Management Console on WACS**.

2. Type the name of your Central Management Server (CMS) in the **System** field.
3. Type your user name and password.

If you're using LDAP or Windows NT authentication, you may log on using an account that has been mapped to the BusinessObjects Enterprise Administrators group.

Note:

If this is the first time an administrator from your organization is accessing the CMC, type Administrator as the user name. This default Enterprise account does not have a password until you create one.

4. Select **Enterprise in the **Authentication Type** list.**

Windows AD, Windows NT and LDAP authentication also appear in the list; however, third-party user accounts and groups must be mapped to BusinessObjects Enterprise before you can use these types of authentication.

5. Click **Log On.**

The CMC Home page appears.

Related Topics

- [Setting the Administrator password](#)

Navigating within the CMC

Because the CMC is a web-based application, you can navigate through it in a number of ways:

- Click the links on the Home page or tabs on the left of your screen to go to specific management areas.
- Select the same management areas from the Navigation list.

Note:

When you are navigating among objects that have many child objects, there may be too many children to display in the tree view. When this happens, you can use the paginated object listing to navigate to the child objects with which you are concerned.

Setting CMC preferences

The "Preferences" area of the CMC allows you to customize your administrative view of BusinessObjects Enterprise.

To set the console preference

1. Log on to the CMC and click **Preferences** in the upper-right corner of the CMC.
2. Set the preference as required.

The Web Intelligence, Desktop Intelligence, Crystal Reports, Dashboard and Analytics, and Change Password preferences work exactly the way they do in InfoView, though they affect the behavior of objects in the CMC as well. For a full explanation of those settings, refer to “Setting Preferences” in the *SAP BusinessObjects Enterprise InfoView User's Guide*.

3. Click **OK**.

Related Topics

- [CMC Preference options](#)

CMC Preference options

CMC Preference option	Explanation
Product Locale	This list sets the default language options for BusinessObjects Enterprise. See the <i>SAP BusinessObjects Enterprise Installation Guide</i> for more information.
Preferred Viewing Locale	This list sets the default formatting options for date, time, and numbers in the CMC.

CMC Preference option	Explanation
Maximum number of objects per page	<p>This option limits the number of objects listed on any page or tab in the CMC.</p> <p>Note: This setting does not limit the number of objects displayed, simply the number displayed per page.</p>
Time Zone	<p>If you are managing BusinessObjects Enterprise remotely, use this list to specify your time zone. BusinessObjects Enterprise synchronizes scheduling patterns and events appropriately. For instance, if you select Eastern Time (US & Canada), and you schedule a report to run at 5:00 a.m. every day on a server that is located in San Francisco, then the server will run the report at 2:00 a.m. Pacific Time.</p>
Prompt for Unsaved Data	<p>This setting controls whether you are prompted for confirmation when you close a dialog box without saving your work by clicking Cancel or by clicking the close button in the top right-hand corner. You have the following options:</p> <ul style="list-style-type: none"> • On: The prompt behavior is enabled. • Off: The prompt behavior is disabled. • Default: The prompt behavior is determined by settings configured in the <code>web.xml</code> file that is located in <code>C:\Program Files\Business Objects\Tomcat55\webapps\Cm-cApp\WEB-INF</code>.

Making initial security settings

Before you publish content or provide users with access to BusinessObjects Enterprise, the default system settings should be changed. This section provides procedures for setting the Administrator password, disabling a user account, and modifying the default security level.

Related Topics

- [How rights work in BusinessObjects Enterprise](#)

Setting the Administrator password

As part of the installation, BusinessObjects Enterprise creates an Administrator account and a Guest account that do not have passwords. Use the following procedure to create a secure password for the Administrator account.

Note:

Do not create a password for the Guest account if you plan to use the anonymous single sign-on or the Sign Up features available in BusinessObjects Enterprise.

To change the Administrator password

1. In the **User Name** field in the CMC log on page, type Administrator.

Note:

This default account does not have a password until you create one.

2. Click **OK**.
3. Go to the "Users and Groups" management area of the CMC.
4. Click **User List**.
5. Select the **Administrator** account, and click **Manage > Properties**.
6. In the "Enterprise Password Settings" area, type and confirm the new password.
7. If it is selected, clear the **User must change password at next logon** check box.
8. Click **Save**.

Disabling a user account

You can disable any user account through the CMC.

For example, you may want to disable the Guest account to ensure that no one can log on to BusinessObjects Enterprise with this account.

Note:

If you disable the Guest account, you also disable the anonymous single sign-on functionality of BusinessObjects Enterprise.

To disable a user account

1. Go to the "Users and Groups" management area of the CMC.
2. Click **User List**.
3. In the **Title** column, select the user account you want to disable and click **Manage** and then **Properties**.
4. Select the **Account is disabled** check box.
5. Click **Save**.

Related Topics

- [Managing Enterprise and general accounts](#)



Setting Rights



18

chapter



How rights work in BusinessObjects Enterprise

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

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

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

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

Related Topics

- [Rights override](#)

Access levels

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

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

However, you can also create and customize your own access levels; this can greatly reduce administrative and maintenance costs associated with security. Consider a situation in which an administrator must manage two groups, sales managers and sales employees. Both groups need to access five reports in the BusinessObjects Enterprise system, but sales managers require more rights than sales employees. The predefined access levels do not meet the needs of either group. Instead of adding groups to each report as principals and modifying their rights in five different places, the administrator can create two new access levels, Sales Managers and Sales Employees. The administrator then adds both groups as principals to the reports and assigns the groups their respective access levels. When rights need to be modified, the administrator can modify the access levels. Because the access levels apply to both groups across all five reports, the rights those groups have to the reports are quickly updated.

Related Topics

- [Working with access levels](#)

Advanced rights settings






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

Use advanced rights settings, for instance, if you need to customize a principal's rights to a particular object or set of objects. Most importantly, use advanced rights to explicitly deny a user or group any right that should not

be permitted to change when, in the future, you make changes to group memberships or folder security levels.

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

Table 18-1: Rights options

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

Related Topics

- [Type-specific rights](#)

Inheritance

Rights are set on an object for a principal in order to control access to the object; however, it is impractical to set the explicit value of every possible right for every principal on every object. Consider a system with 100 rights,

1000 users, and 10,000 objects: to set rights explicitly on each object would require the CMS store billions of rights in its memory, and, importantly, require that an administrator manually set each one.

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

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

BusinessObjects Enterprise recognizes two types of inheritance: group inheritance and folder inheritance.

Group inheritance

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

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

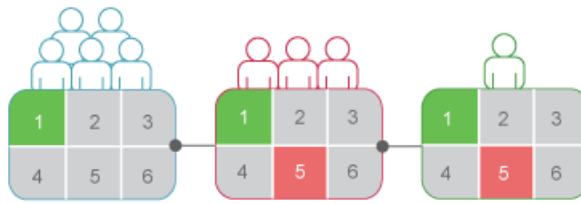


Figure 18-1: Group inheritance example 1

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

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

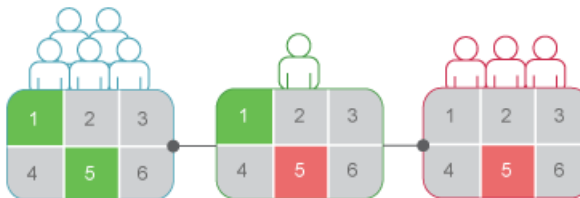


Figure 18-2: Group inheritance example 2

Related Topics

- [Rights override](#)

Folder inheritance

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

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

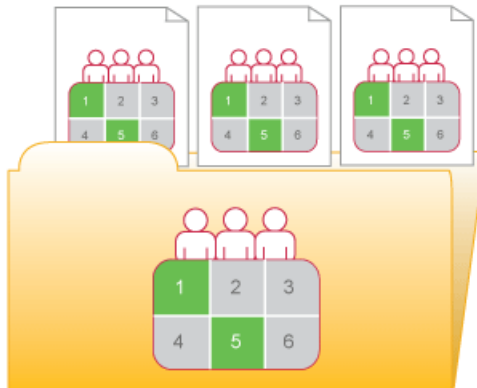


Figure 18-3: Folder inheritance example

Related Topics

- [Rights override](#)

Rights override

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

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

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

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

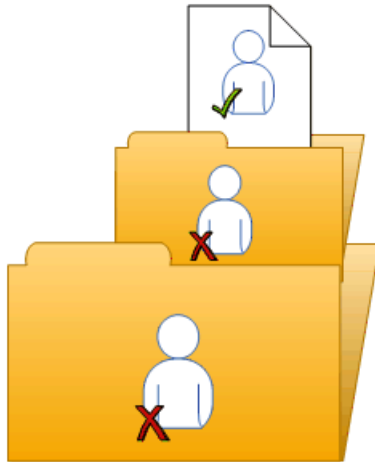


Figure 18-4: Rights override example 1

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

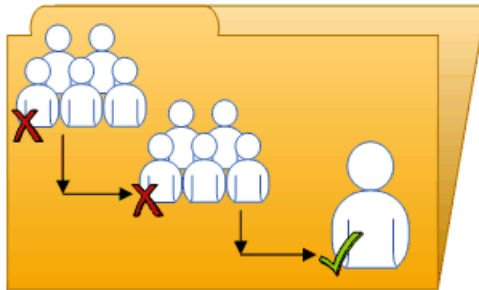


Figure 18-5: Rights override example 2

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

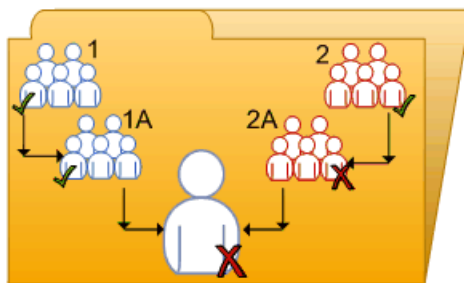


Figure 18-6: Complex rights override

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

Scope of rights

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

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

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

Type-specific rights

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

- General rights for the object type

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

- Specific rights for the object type

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

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

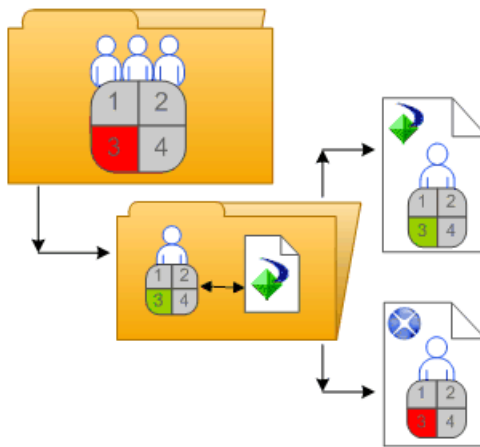


Figure 18-7: Type-specific rights example

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

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

- General

These rights affect all objects.

- Content

These rights are divided according to particular content object types. Examples of content object types include Crystal reports, Adobe Acrobat PDFs, and Desktop Intelligence documents.

- Application

These rights are divided according to which BusinessObjects Enterprise application they affect. Examples of applications include the CMC and InfoView.

- System

These rights are divided according to which core system component they affect. Examples of core system components include Calendars, Events, and Users and Groups.

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

Determining effective rights

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

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

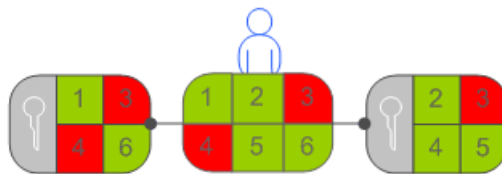


Figure 18-8: Multiple access levels

- Advanced rights can be combined with access levels to customize the rights settings for a principal on an object. For example, if an advanced right and an access level are both assigned explicitly to a principal on an object, and the advanced right contradicts a right in the access level, the advanced right will override the right in the access level.

Advanced rights can override their identical counterparts in access levels only when they are set on the same object for the same principal. For example, an advanced Add right set at the general global level can override the general Add right setting in an access level; it cannot override a type-specific Add right setting in an access level.

However, advanced rights do not always override access levels. For example, a principal is denied an Edit right on a parent object. On the child object, the principal is assigned an access level that grants him the Edit right. In the end, the principal has Edit rights on the child object because the rights set on the child object override rights that are set on the parent object.

- Rights override makes it possible for rights set on a child object to override rights that are inherited from the parent object.

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 BusinessObjects Enterprise.

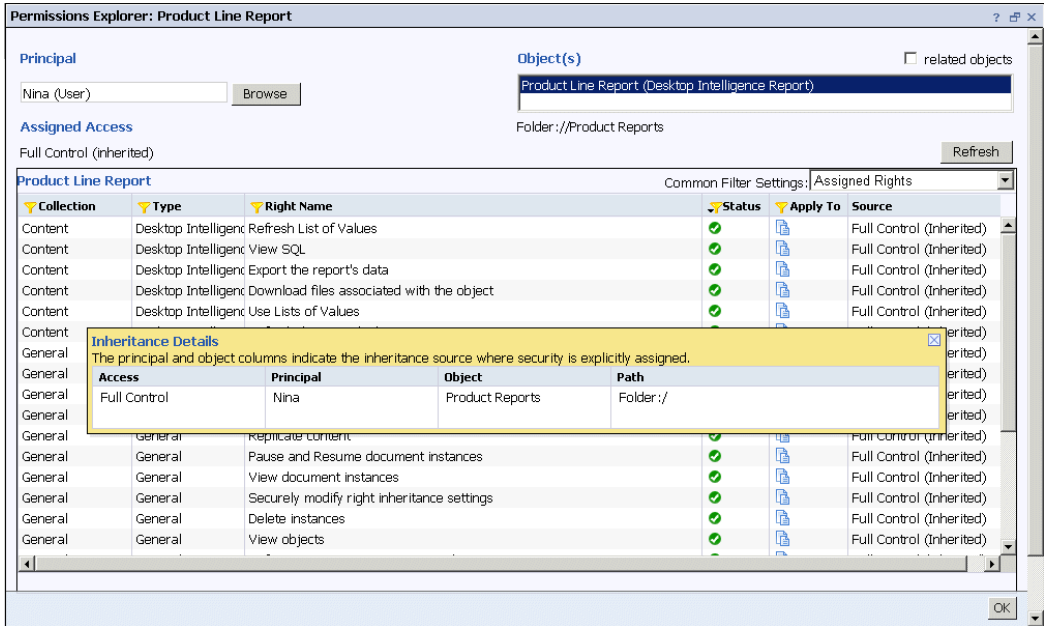
To view rights for a principal on an object

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.

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.

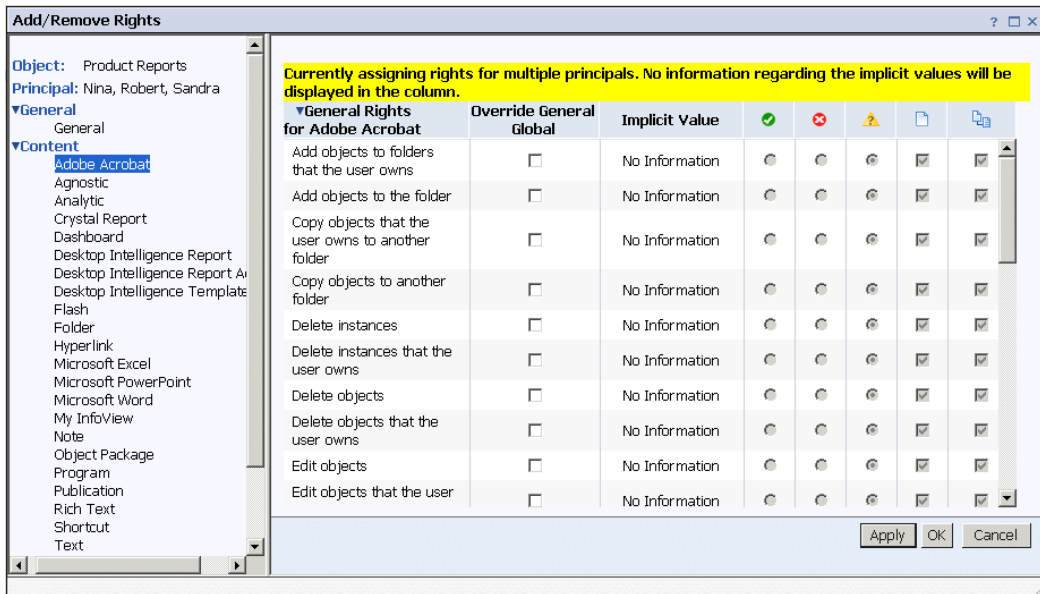
If necessary, you can also modify rights at a granular level to override certain rights in an access level. See [To modify security for a principal on an object](#) for more information.

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.



Related Topics

- [To assign principals to an access control list for an object](#)

To set rights on a top-level folder in BusinessObjects Enterprise

In general, you follow this workflow to set rights on a top-level folder in BusinessObjects Enterprise.

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 Topics

- [To assign principals to an access control list for an object](#)
- [To modify security for a principal on an object](#)

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.

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**.

Create Security Query: Nina

Query Principal

This query will search for objects for the following principal:

Nina

Query Permission

This query will search for objects where the above principal has all of the following permissions:

☐ Do not query by permissions

Collection	Type	Right Name		
General	General	Add objects to folders that the user owns	✓	<input type="button" value="X"/>
General	General	Add objects to the folder	✓	<input type="button" value="X"/>

Query Context

This query will search for objects in the following section(s) of the CMC only:

☒ Folders

(All) ☒ Query sub object

☐ Folders

(All) ☐ Query sub object

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.

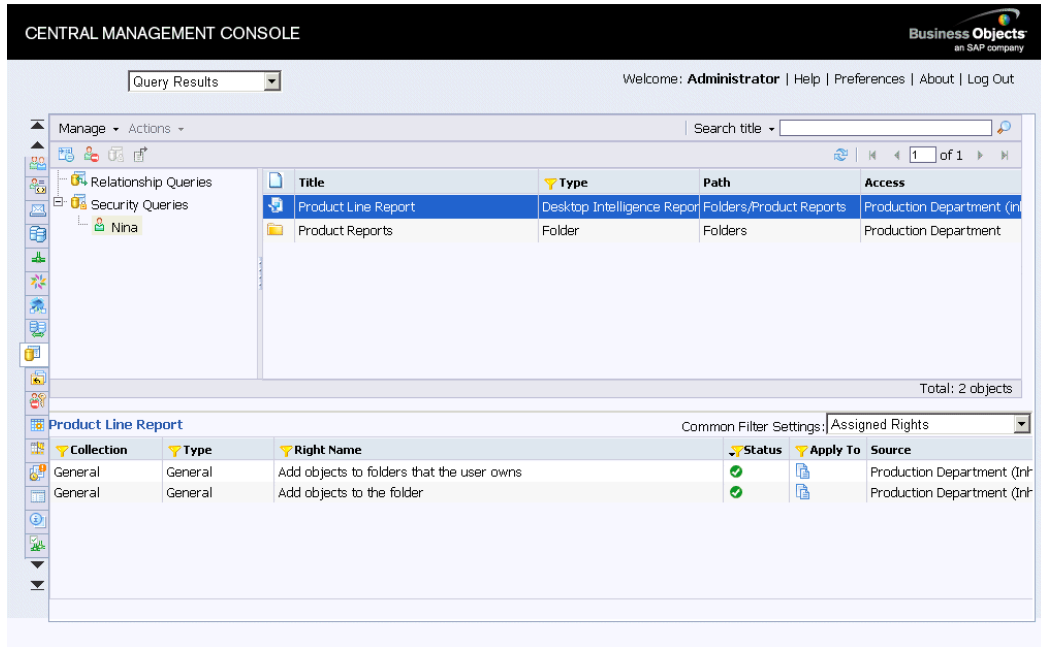
When you do this, BusinessObjects Enterprise runs a general security query for all objects that have the principal in their access control lists regardless of the permissions that the principal has on the objects.

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

Note:

You can query a maximum of four areas.

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



Tip:

Query results are listed according to the names of principals.

The query results are displayed in the Details panel.

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.

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 BusinessObjects Enterprise to set rights quickly and uniformly for many principals.

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

Table 18-2: 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.	<ul style="list-style-type: none">• View objects• View document instances

Access level	Description	Rights involved
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Refresh the report's data
Full Control	A principal has full administrative control of the object.	All available rights, including: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> Add right on the Access Levels top-level folder
View granular rights in an access level	<ul style="list-style-type: none"> View right on the access level
Assign an access level to a principal on an object	<ul style="list-style-type: none"> 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 <p>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.</p>
Modify an access level	<ul style="list-style-type: none"> View and Edit rights on the access level
Delete an access level	<ul style="list-style-type: none"> View and Delete rights on the access level
Clone an access level	<ul style="list-style-type: none"> View right on the access level Copy right on the access level Add right on the Access Levels top-level folder

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, BusinessObjects Enterprise 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.

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.

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.

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.

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**.

Note:

You cannot delete predefined access levels.

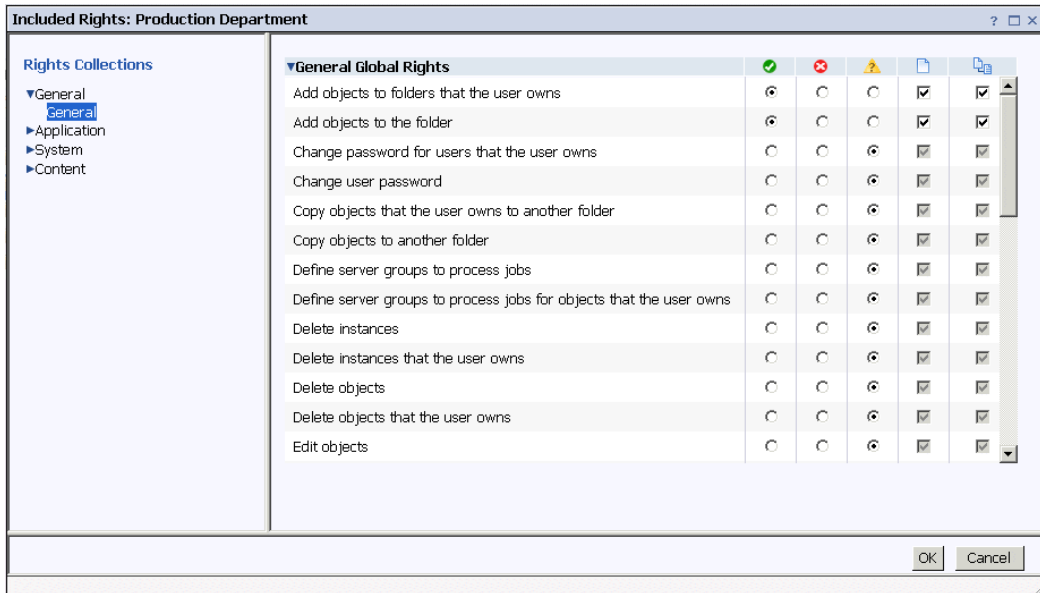
A dialog box appears with information about the objects that this access level affects. If you do not want to delete the access level, click **Cancel** to exit the dialog box.

3. Click **Delete**.
The access level is deleted, and you return to the "Access Levels" area.

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.

Related Topics

- [Managing security settings for objects in the CMC](#)
- [Type-specific rights](#)

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.
- 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.

Related Topics

- [Relationships](#)

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 Topics

- [Federation](#)
- [Relationships](#)

Breaking inheritance

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

Note:

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

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

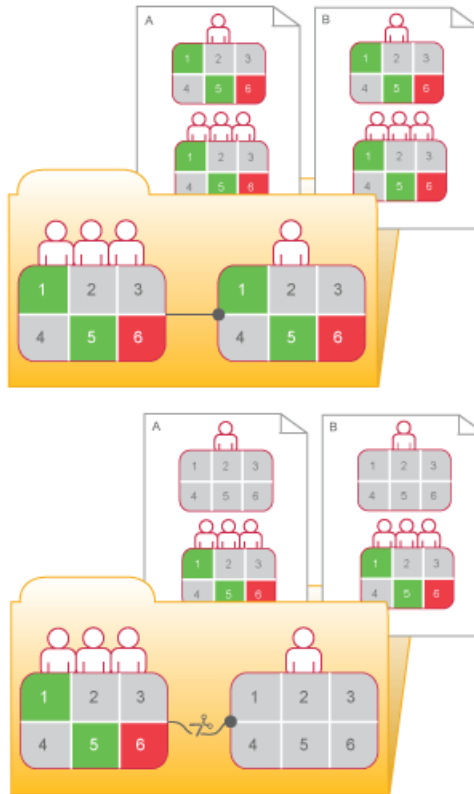


Figure 18-9: Breaking inheritance

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**.

Using rights to delegate administration

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

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

Note:

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

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

Table 18-3: Rights for delegated administrators

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

Action for delegated administrator	Rights required by the delegated administrator
Modify passwords only for principals the delegated administrator creates	Owner Edit Password right on top-level Users folder, or on relevant groups Note: Setting the Owner Edit Password right on a group takes effect on a user only when you add the user to the relevant group.
Modify user names, description, other attributes, and reassign users to different groups	Edit right on relevant groups
Modify user names, description, other attributes, and reassign users to different groups, but only for users that the delegated administrator creates	Owner Edit right on top-level Users folder, or on relevant groups Note: Setting the Owner Edit right on relevant groups takes effect on a user only when you add the user to the relevant group.

Choosing between “Modify the rights users have to objects” options

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

Rights Inheritance Settings right. The differences between these rights are summarized below.

Modify the rights users have to objects

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

Securely modify the rights users have to objects

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

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

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

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

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

Securely modify rights inheritance settings

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

Owner rights

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

Owner rights are useful in managing owner-based security. For example, you may want to create a folder or hierarchy of folders in which various users can create and view documents, but can only modify or delete their own documents. In addition, owner rights are useful for allowing users to manipulate instances of reports they create, but not others' instances. In the case of the scheduling access level, this permits users to edit, delete, pause and reschedule only their own instances.

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

Summary of recommendations for rights administration

Keep these considerations in mind for rights administration:

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



Managing Users and Groups

19

chapter



Account management overview

Account management can be thought of as all of the tasks related to creating, mapping, changing, and organizing user and group information. The "Users and Groups" management area of the Central Management Console (CMC) provides you with a central place to perform these tasks.

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

User management

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

Table 19-1: Default user accounts

Account name	Description
Administrator	This user belongs to the Administrators and Everyone groups. An administrator can perform all tasks in all BusinessObjects Enterprise applications (for example, the CMC, CCM, Publishing Wizard, and InfoView).

Account name	Description
Guest	<p>This user belongs to the Everyone group. This account is enabled by default, and is not assigned a password by the system. If you assign it a password, the single sign-on to InfoView will be broken.</p> <p>See the <i>SAP BusinessObjects Enterprise Administrator's Guide</i> for information on supporting Guest users in multiple time zones.</p>

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.

Group management

Groups are collections of users who share the same account privileges; therefore, you may create groups that are based on department, role, or location. Groups enable you to change the rights for users in one place (a group) instead of modifying the rights for each user account individually. Also, you can assign object rights to a group or groups.

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

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

Table 19-2: Default group accounts

Account name	Description
Administrators	Members of this group can perform all tasks in all of the BusinessObjects Enterprise applications (CMC, CCM, Publishing Wizard, and InfoView). By default, the Administrators group contains only the Administrator user.
Everyone	Each user is a member of the Everyone group.
QaaWS Group Designer	Members of this group have access to Query as a Web Service.
Report Conversion Tool Users	Members of this group have access to the Report Conversion Tool application.
Translators	Members of this group have access to the Translation Manager application.
Universe Designer Users	Users who belong to this group are granted access to the Universe Designer folder and the Connections folder. They can control who has access rights to the Designer application. You must add users to this group as needed. By default, no user belongs to this group.

Related Topics

- [How rights work in BusinessObjects Enterprise](#)
- [Granting access to users and groups](#)

Available authentication types

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

Table 19-3: Authentication types

Authentication type	Description
Enterprise	Use the system default Enterprise Authentication if you prefer to create distinct accounts and groups for use with BusinessObjects Enterprise, or if you have not already set up a hierarchy of users and groups in a Windows NT user database, an LDAP directory server, or a Windows AD server.

Authentication type	Description
Windows NT	If you are working in a Windows NT environment, you can use existing NT user accounts and groups in BusinessObjects Enterprise. When you map NT accounts to BusinessObjects Enterprise, users are able to log on to BusinessObjects Enterprise applications with their NT user name and password. This can reduce the need to recreate individual user and group accounts within BusinessObjects Enterprise.
LDAP	If you set up an LDAP directory server, you can use existing LDAP user accounts and groups in BusinessObjects Enterprise. When you map LDAP accounts to BusinessObjects Enterprise, users are able to access BusinessObjects Enterprise applications with their LDAP user name and password. This eliminates the need to recreate individual user and group accounts within BusinessObjects Enterprise.

Authentication type	Description
Windows AD	If you are working in a Windows 2000 environment, you can use existing AD user accounts and groups in BusinessObjects Enterprise. When you map AD accounts to BusinessObjects Enterprise, users are able to log on to BusinessObjects Enterprise applications with their AD user name and password. This eliminates the need to recreate individual user and group accounts within BusinessObjects Enterprise.

Note:

You can use Enterprise Authentication in conjunction with either NT, LDAP, or AD authentication, or with all of the three authentication plug-ins.

For more information, see the *SAP BusinessObjects Enterprise Deployment and Configuration Guide*.

Managing Enterprise and general accounts

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

Note:

- In many cases, these procedures also apply to NT, LDAP, and AD account management. For specific information on NT, LDAP, and AD authentication, see the *SAP BusinessObjects Enterprise Administrator's Guide*.
- When a user logs off their web session on BusinessObjects Enterprise by navigating to a non-BusinessObjects Enterprise page or closing their

web browser, their Enterprise session is not logged off and they still hold 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 BusinessObjects Enterprise.

To create an Enterprise 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. Select **Enterprise** from the **Authentication Type** list.
4. Type the account name, full name, email, and description information.

Tip:

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

5. Specify the password information and settings.
6. Select the connection type.
 - Choose **Concurrent User** if this user belongs to a license agreement that states the number of users allowed to be connected at one time.
 - Choose **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 BusinessObjects Enterprise regardless of the number of other people who are currently connected.
7. 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, as is an Enterprise alias. You can now add the user to a group or specify rights for the user.

Related Topics

- [How rights work in BusinessObjects Enterprise](#)

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 Topics

- [To create a new alias for an existing user](#)

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.

Note:

Deleting a user account won't necessarily prevent the user from being able to log on to BusinessObjects Enterprise 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 BusinessObjects Enterprise, 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.

4. Click **OK**.

The user account is deleted.

Related Topics

- [To modify a user account](#)
- [To delete a user account](#)
- [To disable an alias](#)

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 BusinessObjects Enterprise content.

To modify a group's properties

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

Note:

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

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**.

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.

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 an NT user database, LDAP user directory, or AD user directory.

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

To add subgroups

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

Note:

Adding a subgroup is similar to specifying group membership.

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 Topics

- [To specify group membership](#)

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.

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.
- 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 BusinessObjects NT Users group, use the "Authentication" management area in CMC. For instructions, see the *SAP BusinessObjects Enterprise Deployment Planning Guide*.

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.

To enable the Guest account

The Guest account is disabled by default to ensure that no one can log on to BusinessObjects Enterprise with this account. This default setting also disables the anonymous single sign-on functionality of BusinessObjects Enterprise, so users will be unable to access InfoView 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 InfoView.

1. Go to the "Users and Groups" management area of the CMC.
2. Click **User List** in 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**.

Adding users to groups

You can add users to groups in the following ways:

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

The following procedures describe how to add users to groups using these methods.

Related Topics

- [To specify group membership](#)

To add a user to one or more groups

1. Go to the "Users and Groups" management area of the CMC.
2. Select the user that you want to add to a group.
3. Click **Actions > Join Group**.

Note:

All BusinessObjects Enterprise users of the system are part of the Everyone group.

The "Join Group" dialog box appears.

4. Move the group that you want 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.

5. Click **OK**.

To add one or more users to a group

1. In the "Users and Groups" management area of the CMC, select the group.
2. Click **Actions > Add Members to Group**.
The "Add" dialog box appears.
3. Click **User list**.
The **Available users/groups** list refreshes and displays all user accounts in the system.
4. Move the user that you want to add to the group from the **Available users/groups** list to the **Selected users/groups** list.

Tip:

- To select multiple users, use the **SHIFT + click** or **CTRL + click** combination.
 - To search for a specific user, use the search field.
 - If there are many users on your system, click the Previous and Next buttons to navigate through the list of users.
5. Click **OK**.

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 (Windows NT, LDAP, or Windows AD). Generally, however, your external system will enable you to place similar restrictions on the external accounts.

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 wish to change.

The available options are:

- **Password never expires**
- **User must change password at next logon**
- **User cannot change password**

5. Click **Save & Close**.

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.

Table 19-4: Password settings

Password setting	Minimum	Recommended Maximum
Enforce mixed-case passwords	N/A	N/A
Must contain at least N Characters	0 characters	64 characters
Must change password every N day(s)	1 day	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

4. Click **Update**.

Enabling Trusted Authentication

Note:

Trusted Authentication is supported for InfoView 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 BusinessObjects Enterprise 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.

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.

Note:

The shared secret is used by the client and the CMS to create a trusted authentication password. This password is used to establish trust.

5. Enter a time-out value for your trusted authentication requests.

Note:

The time-out value determines how long the CMS waits for the `ILogonSession.logon()` call from the client application.

6. Click **Update**.

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:

```
ILogonMgr sessionMgr = CrystalEnterprise.getSessionMgr();
```

```
ITrustedPrincipal trustedPrincipal = sessionMgr.createTrustedPrincipal("userName", "cmsName");  
IEnterpriseSession enterpriseSession = sessionMgr.login(trustedPrincipal);
```

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 Topics

- [To assign principals to an access control list for an object](#)

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 Topics

- [Selecting a destination](#)
- [To send an object or an instance to a destination](#)
- [Managing security settings for objects in the CMC](#)

Configuring the InfoView logon screen

By default, the InfoView logon screen prompts users for their user name and password. You can also prompt them for the CMS name and the authentication type. To change this setting, you need to edit the `InfoViewweb.xml` file.

To configure the InfoView logon screen in the `web.xml` file

1. Open the `web.xml` file for InfoView from its deployed location on your web application server.

The `InfoViewweb.xml` file is stored in the following location on Windows:

Deployed Location\Business Objects\BusinessObjects
Enterprise 12.0\warfiles\WebApps\InfoViewApp\WEB-INF.

Note:

- If you are using the version of Tomcat installed with BusinessObjects Enterprise on Windows, and you did not modify the default installation location, replace *Deployed Location* with `C:\Program Files`.
- If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path.

2. To prompt users for the authentication type on the logon screen, locate the `authentication.visible` parameter and change its `<param-value>` from `false` to `true`:

```
<param-value>true</param-value>
```

3. To change the default authentication type, locate the `authentication.default` parameter and change its `<param-value>` to one of the following:

Authentication Type	Parameter Value
Enterprise (default)	<code><param-value>secEnterprise</param-value></code>
LDAP	<code><param-value>secLDAP</param-value></code>
AD	<code><param-value>secWinAD</param-value></code>

4. To prompt users for the CMS name on the logon screen, locate the `cms.visible` parameter and change its `<param-value>` from `false` to `true`:

```
<param-value>true</param-value>
```

5. Save and close the file.
6. Restart your web application server.

Managing aliases

If a user has multiple accounts in BusinessObjects Enterprise, 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 BusinessObjects Enterprise, LDAP, AD, or NT aliases.

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 BusinessObjects Enterprise 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 BusinessObjects Enterprise.
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 NT.

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 BusinessObjects Enterprise and is assigned an alias for the authentication type you selected, for example, secWindowsNT:ENTERPRISE:bsmith. If required, you can add, assign, and reassign aliases to users.

To create a new alias for an existing user

You can create aliases for existing BusinessObjects Enterprise 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 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 BusinessObjects Enterprise.
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 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.

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**.

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.

Note:

Deleting a user's alias does not necessarily prevent the user from being able to log on to BusinessObjects Enterprise again. If the user account still exists in the third-party system, and if the account belongs to a group that is mapped to BusinessObjects Enterprise, then BusinessObjects Enterprise 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.

To disable an alias

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

Note:

Deleting a user from BusinessObjects Enterprise does not necessarily prevent the user from being able to log on to BusinessObjects Enterprise again. If the user account still exists in the third-party system, and if the account belongs to a group that is mapped to BusinessObjects Enterprise, then BusinessObjects Enterprise 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 BusinessObjects Enterprise, 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 Topics

- [To delete an alias](#)



Managing Applications

20

chapter



Overview

The "Applications" area of the CMC allows you to change the appearance and functionality of web applications such as the CMC, Desktop Intelligence and InfoView, 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 how to manage various settings. The following applications are available for modification:

- BI Widgets
- CMC settings
- Content Search
- Designer
- Desktop Intelligence
- Discussions
- Encyclopedia
- InfoView
- Performance Management
- Report Conversion Tool
- Strategy Builder
- Web Intelligence

Setting user rights on applications

You can use rights to control user access to certain features in BusinessObjects Enterprise applications.

Note:

- User rights settings are not available for the Discussions application. However, you can set rights on individual reports.
- For the Web Intelligence application, make sure you grant users the **Enable interactive HTML viewing (if license permits)** right so that they can use the interactive view format and the Query HTML panel. In InfoView, the user can select this view format and report panel option by clicking **Preferences** and expanding **Web Intelligence**.

Related Topics

- [Managing security settings for objects in the CMC](#)

Managing Discussions settings

To manage Discussions settings in the CMC

BusinessObjects Enterprise administrators are responsible for maintaining discussion threads for BusinessObjects Enterprise users.

1. Go to the "Applications" area of the CMC and select **Discussions**.
2. Click **Manage > Properties**.

The "Notes Administration" dialog box opens and lets you manage, search and sort through discussion threads.

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 > Properties**.

The **Notes Administration** dialog box opens.

3. In the **Field name** list, select an option.

Option	Description
Thread title	Searches by thread title.
Creation date	Searches by creation date.
Last modified date	Searches by the last date modified.
Author	Searches by author.

4. On the second list, refine your search.

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**.

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 > Properties**.

The "Notes Administration" dialog box opens.
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**.

To delete a discussion thread

You can delete any discussion thread in the "Applications" area of the CMC in BusinessObjects Enterprise.

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

Setting user rights

User rights settings are not available for the Discussions application. However, you can allow users to have rights on individual reports in order to create a discussion thread, or add a note to a report.

Related Topics

- [Managing security settings for objects in the CMC](#)

Managing InfoView settings

In the "Applications" area of the CMC in BusinessObjects Enterprise, you can change the display options of InfoView by going to **Manage > Properties**.

For InfoView, you can grant users or groups the ability to:

- Change preferences
- Organize folders
- Search
- Filter object listings by object type
- View the Favorites folder

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

Note:

By default, all users have access to these features.

To change display settings for InfoView

1. Go to the "Applications" area of the CMC and select **InfoView**.
2. Click **Manage > Properties**.
The "Infoview Properties" dialog box opens.
3. Set the appropriate options.

Option	Description
"Header and style"	<p>Change the colors of the header and the logo displayed in the header to match your brand or use the BusinessObjects logo and colors. If you have a cascading style sheet for your Intranet, specify it here to format InfoView with the same styles.</p> <p>Tip: When you are creating a cascading style sheet, it is recommended that you make a copy of the default CSS file installed with InfoView and make necessary changes to the copy instead of creating an entirely new CSS. The <code>default.css</code> file can be found in <code>[install_dir]\Business Objects\Tomcat55\webapps\InfoViewApp\res\schema.blue</code>.</p>
"Display"	Choose the functionality that your users can see. Select whether or not to display the Preferences button, the Type list, and the Filters tab.
"Default Navigation View"	Choose a navigation method for your users. The choices are Folder or Category .
"Default Viewing Action on Listing Page"	Configure settings to control whether double-clicking the report opens the object or the latest successful instance of the object.

4. Click **Save & Close**.

Managing Web Intelligence settings

You can control which interactive features your users have access to for Web Intelligence documents by setting its properties from the "Applications" area of the CMC.

Note:

To allow users to use the interactive view format and the Query HTML panel, you must grant them the **Enable interactive HTML viewing (if license permits)** right. In InfoView, users can select this view format and report panel option by clicking **Preferences** and expanding **Web Intelligence**.

To modify display settings in Web Intelligence

1. Go to the "Applications" area of the CMC and select **Web Intelligence**.
2. Click **Manage > Properties**.
The "Properties" dialog box opens with display options.
3. Define the display options that you want.

Option	Description
"Dimensions and de-tails"	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.
"Data Synchronization Options"	To prevent automatic merging of dimentions even when auto-merge criteria exist, de-select the Auto-Merge dimensions option.

4. Click **Save & Close**.

Note:

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

Managing BI Widgets settings

BI Widgets is a new desktop application located in the CMC area of BusinessObjects Enterprise. It is designed to provide you with a simple, intuitive deployment architecture from the CMC. Like other BusinessObjects Enterprise applications, BI Widgets allows you to modify general as well as advanced user rights.

Using the "Applications" area of the CMC, you can grant users or groups the ability to:

- Use BI Widgets
- Edit BI Widgets objects
- Modify user rights to a BI Widget object

Note:

By default, all general users have access to these features.

Related Topics

- [Managing security settings for objects in the CMC](#)

Managing Polestar settings

You can define which features your users have access to for Polestar by settings its security rights from the Applications area of the CMC.

Related Topics

- [Managing security settings for objects in the CMC](#)
- [Polestar](#)

To modify Polestar application properties

1. Go to the "Applications" area of the CMC.
2. Click **Manage > Properties**.
The "Polestar Properties" dialog box appears.
3. Define the Polestar settings that you want.

- Default index folder location
- Number of threads
- Bookmark validity

4. Click **Save & Close**.



Managing Data Sources and Connections



21

chapter

Overview

This section provides information to help you manage data sources and connections, including information on the following topics:

- [Data source connections](#)
- [Managing universes](#)

Note:

For more information about Voyager connections, please refer to the *BusinessObjects Voyager Administrator's Guide*.

Data source connections

Before data analysts begin working with business data, they must create connections to your universes and add them to their workspaces.

A connection is a BusinessObjects Enterprise repository object that contains all the information required for a Query and Analysis product, such as Voyager, to connect to a data source. By using this connection method, you can:

- Improve security

Only administrators and users who have privileges to add objects to the BusinessObjects Enterprise repository need to know server details. Also, connection details such as server name, database, username, and password are stored in the repository, not in workspace files.

- Enhance productivity

Organizations can easily move workspaces between development and production environments by storing connection information in a shared connection object. Instead of changing all the workspaces, you can modify only the shared connection object to reference the production server instead of the development server. The updated connection information is automatically sent to the workspaces that reference the shared connection object.

Managing universes

A universe is an abstraction of a data source that contains data in non-technical terms. Users of Web Intelligence can connect to a universe and run queries through it against a database. They can perform data analysis and create reports using the objects in a universe without seeing, or knowing anything, about the underlying data structures in the database. Universes are created by using the Universe Designer.

You can grant user access to universes and allow people to create and view documents that use universes and connections.

Related Topics

- [Managing security settings for objects in the CMC](#)

To delete universes

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**.

Managing universe connections

To delete a universe connection

Tip:

It is also possible to delete connections in Universe Designer.

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

Controlling access to universe connections

You can grant user access to universe connections and allow users to create and view documents that use universes and connections.

Related Topics

- [*Managing security settings for objects in the CMC*](#)



Working with Content Objects

22

chapter



Overview

This section describes the management of objects using the CMC. It includes general information that applies to all objects, and it includes specific information about managing reports, Web Intelligence documents, programs, and object packages.

This section covers the following topics:

- [General object management](#)
- [Report object management](#)
- [Program object management](#)
- [Object package management](#)

General object management

Many objects can exist in BusinessObjects Enterprise, including reports, Web Intelligence documents, programs, Microsoft Excel files, Microsoft Word files, Microsoft PowerPoint files, PDFs, rich text format files, text files, and hyperlinks, as well as object packages, which consist of report and/or program objects. After adding objects to BusinessObjects Enterprise, you manage them through the Central Management Console (CMC) by going to the "Folders" management area.

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.

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.

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. In the "Select destination(s)" area, browse for the folder that you want to move the object to.

Note:

In order to complete this task successfully, you must select the folder in the details pane on the right side.

Tip:

Use **SHIFT + click** or **CTRL + click** to select multiple folders.

4. Click **>** to move the folder or folders to the **Destinations** list.
5. Click **Move**.
The object moves from the origin folder to the destination folder.

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.

To delete an object

This procedure explains how to delete either a single object or multiple objects. You can also delete a folder, which deletes all of the objects and instances that are stored in that folder. As well, you have the option of deleting 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**.

Related Topics

- [Managing and viewing the history of instances](#)

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 all fields.

- **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.

To send an object or an instance to a destination

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.

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 or Inbox. Not all types of objects can be sent to all destinations.

1. Go to the "Folders" management area of the CMC.
2. Select the object that you want to send.

Tip:

Use **SHIFT + click** or **CTRL + click** to select multiple objects.

To send an instance of the object, select the object in the Navigation panel so that its instances are displayed in the Details panel. Select the instances 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.

3. Click **Organize** > **Send** and click the destination option that you want.

Note:

Send Web Intelligence documents to the Inbox destination only, or to an Email destination configured within BusinessObjects Enterprise.

Option	Description
Business Objects Inbox	Sends the object to a user's InfoView inbox.
Email	Sends the object to a user's email address.
FTP Location	Sends the object to an FTP server location.
File Location	Sends the object to a local disk location.

A dialog box appears and lets you configure the destination option you chose. The options in the dialog box vary depending on the destination option.

4. Configure your destination option.

You can choose to use the Destination 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 an Inbox destination 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 server).

5. When you are finished, click **Submit**.

Related Topics

- [Available destinations by object type](#)

Available destinations by object type

Most destinations can be used for most types of objects, but there are some exceptions. In some cases recipients must have access to the BusinessObjects Enterprise system to be able to open the object.

Object type	Unm. Disk	FTP	Email (SMTP)		Inbox	
			File	Link	File	Link
Report	Yes	Yes	Yes	Yes	Yes	Yes
Object Package	-	-	-	-	Yes	Yes
Program	Yes	Yes	Yes	Yes	Yes	Yes
Web Intelligence document	Yes	Yes	Yes	Yes	Yes	Yes
Desktop Intelligence document	Yes	Yes	Yes	Yes	Yes	Yes
Voyager workspace	-	-	-	Yes	Yes	Yes
Excel file	Yes	Yes	Yes	Yes	Yes	Yes

Object type	Unm. Disk	FTP	Email (SMTP)		Inbox	
			File	Link	File	Link
Word file	Yes	Yes	Yes	Yes	Yes	Yes
PDF file	Yes	Yes	Yes	Yes	Yes	Yes
Text file	Yes	Yes	Yes	Yes	Yes	Yes
RTF file	Yes	Yes	Yes	Yes	Yes	Yes
Power-Point file	Yes	Yes	Yes	Yes	Yes	Yes
Hyperlink	-	-	-	Yes	Yes	Yes

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**.

To assign an object to a category

Like folders, categories are objects used to organize documents. You can associate objects with multiple categories, or subcategories within categories. A category can be a corporate or a personal category.

Use the following procedure to assign an object to a category by using the objects page. You can also assign objects to a category by using the categories page.

1. In the "Folders" management area of the CMC, select an object.
2. Click **Manage > Categories**.
3. Select the category you want to add the object to.
Selected categories are blue.
4. When you are finished, click **Save & Close**.

Related Topics

- [Working with categories](#)
- [To add an object to a category](#)
- [To remove or delete objects from a category](#)

Relationships

In BusinessObjects Enterprise, objects are related to one another in several ways. Folders are related to their children, connections are related to the universes that use them, and reports and documents are related to universes.

The interrelation of objects in BusinessObjects Enterprise can make it difficult to change an object because doing so may break links to the object. You can find out which objects are directly related by performing a relationship query.

Consider a company where a database is being replaced by a new database in a different location. The administrator must find out which objects depend on the current connection so that these objects can be edited accordingly. Then, the database connection can be deleted without causing a disruption to the content of any objects. The administrator runs a relationship query on

the connection, which returns a list of universes that use the connection. All the universes can then be updated.

However, the company has instead decided to delete all the objects that depend on that connection. The administrator runs further relationship queries on all of the universes that were returned by the first query. All objects that use those universes are returned.

Relationship queries can be performed in the following areas of the CMC:

- "Folders"
- "Personal Folders"
- "Categories"
- "Personal Categories"
- "Users and Groups"
- "Profiles"
- "Universes"
- " Access Levels"
- "Servers"
- "Replication Lists"

After you perform the relationship query, you arrive at the "Query Results" area, where the results of your query are displayed. From the "Query Results" area, you can perform basic object management tasks on result objects.

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.

Report object management

Managing report objects includes applying processing extensions, specifying alert notification, changing database information, updating parameters, using filters, and working with hyperlinked reports. This section explains report objects and instances, and how to manage them through the Central Management Console (CMC).

Note:

Most information in this section also applies to Web Intelligence document objects. Any exceptions have been identified.

What are report objects and instances?

A report object is an object that is created using a Business Objects designer component (such as Crystal Reports or Voyager). A Web Intelligence document object is created using the Report panel and HTML Query panel in InfoView. Both types of objects contain report information (such as database fields). Both types of objects can also contain saved data.

A report object or Web Intelligence document object can be made available to everyone or to individuals in selected user groups.

Scheduled instances

When you schedule an object, the system creates a scheduled instance for the object. A scheduled instance contains object and schedule information. It does not contain any data yet. Scheduled instances appear in the History for the respective object and have a status of Recurring or Pending.

You can schedule objects from the CMC or by using a BusinessObjects Enterprise application, such as InfoView, or a custom web application.

Typically, report objects are designed such that you can create several instances with varying characteristics. For example, if you run a report object with parameters, you can schedule one instance that contains report data that is specific to one department and schedule another instance that contains information that is specific to another department, even though both instances originate from the same report object.

Object instances

At the specified time, the system runs the object and creates an object instance. The instance contains actual data from the database. It appears in the History for the object and has a status of Success or Failed.

Changing default settings for an object

Any changes you make to an object affect the default settings for the object only. Those changes do not affect any existing scheduled instances or object instances. The next time you schedule the object, whether you use CMC or an application such as InfoView, the new default settings are displayed. You can then change these settings as needed for the scheduled instance you want to create.

Note:

BusinessObjects Enterprise supports reports created in versions 6 through 2008 of Crystal Reports. Once published to BusinessObjects Enterprise, reports are saved, processed, and displayed in version 2008 format.

Related Topics

- [Scheduling](#)

Setting report refresh options

Note:

This feature applies to Crystal reports only.

You can set report refresh options that determine which settings of a report object are updated when you refresh it in BusinessObjects Enterprise.

When you refresh a report object, BusinessObjects Enterprise compares the report object stored in BusinessObjects Enterprise with the original .rpt file stored in the Input File Repository Server. BusinessObjects Enterprise deletes or adds report elements in the report object to make it match the .rpt file, overwriting any changes you've made in BusinessObjects Enterprise. Where report elements are the same in the source report and the report object, the report refresh settings allow you to control which settings in the report object are updated with values from the source .rpt file.

For example, if a prompt appears only in the source .rpt file, then refreshing the report adds the prompt to the report object. This holds true no matter which report refresh options you select.

If a prompt appears in both the source .rpt and the report object and you have selected the **Current and default parameter values** option, then BusinessObjects Enterprise updates the default value of the prompt in the report object. Any changes that you have made to the default value of the parameter in BusinessObjects Enterprise are overwritten.

To preserve your changes to the values of report elements when you refresh a report, clear the appropriate report refresh option.

- If you select **Current and default parameter values**, BusinessObjects Enterprise ensures that changes to either the default value of a prompt or to the current value of a prompt are updated in the report object when the report is refreshed.
- If you select **Use Object Repository when refreshing report**, repository objects in the report object will be refreshed against the repository. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To set a report object's refresh options

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Actions > Refresh Options**.
The "Refresh Options" dialog box appears.
3. Choose the report elements that you want to refresh from the source report file.
4. Click **Update**.

Tip:

Alternatively, you can click **Refresh report** to immediately refresh the report according to your specifications.

Setting report processing options

Setting report viewing options

Note:

This feature does not apply to Web Intelligence or Desktop Intelligence documents.

The report viewing options available in BusinessObjects Enterprise allow you to balance users' need for up-to-date information with the need to optimize data retrieval times and overall system performance.

BusinessObjects Enterprise allows you to enable data sharing, which permits different users accessing the same report object to use the same data when viewing or refreshing a report. Enabling data sharing reduces the number of database calls, thereby reducing the time needed to generate a report instance for subsequent users of the same report, while greatly improving overall system performance under load.

You can control data sharing settings on either a per-report or a per-server basis:

- If you specify which servers a report uses for viewing, you can use per-server settings to standardize data sharing settings for groups of reports, and centrally administer these settings.
- Per-report settings permit you to specify that particular reports will not share data. They also allow you to tailor the data sharing interval for each report to meet the needs of that report's users. In addition, per-report settings enable you to decide on a report-by-report basis whether it is appropriate to allow users to access the database whenever they refresh reports.

Data sharing may not be ideal for all organizations, or for all reports. To get full value from data sharing, you must permit data to be reused for some period of time. This means that some users may see “old” data when they view a report on demand, or refresh a report instance that they are viewing.

The default report viewing options for BusinessObjects Enterprise emphasize data freshness and integrity. By default, when you add a report to BusinessObjects Enterprise it is configured to use per-server settings for

report sharing. The default server settings ensure that users always receive up-to-date information when they refresh a report, and guarantee that the oldest data given to any user is 0 minutes old. If you choose to enable per-report settings, the default settings allow data sharing, allow a viewer refresh to retrieve fresh data from the database, and ensure that the oldest data given to a client is 5 minutes old.

Tip:

Disabling the sharing of report data between clients is not the same as setting **Oldest on-demand data given to a client** to 0 minutes. Under high load, your system may receive more than one request for the same report instance at the same time. In this case, if the data sharing interval is set to 0 but the **Share report data between clients** option is enabled, BusinessObjects Enterprise shares data between the client requests. If it is important that data not be shared between different clients (for example, because the report uses a User Function Library (UFL) that is personalized for each user), disable data sharing for that report.

For details on setting report viewing options on a per-server basis, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

For more information on configuring BusinessObjects Enterprise to optimize report viewing in your system, see the planning section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

Related Topics

- [Specifying default servers](#)

To set report viewing options for a report

1. In the "Folders" management area of the CMC, select a report.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Viewing Server Group** on the navigation list.
4. In the "Data Refresh for Viewing" area, click **Use report specific viewing settings**, and then select the options that you want to set for this report.
5. Click **Save & Close**.

Specifying default servers

You can specify the default servers that BusinessObjects Enterprise will use to run an object, and to schedule and process instances. For report objects and Web Intelligence documents, you can specify the default servers that BusinessObjects Enterprise will use when a user views or modifies a report or Web Intelligence document. For Desktop Intelligence documents, you can specify the default servers that BusinessObjects Enterprise will use when processing and caching documents.

When specifying your servers, you have three options:

- **Use the first available server**

BusinessObjects Enterprise will use the server that currently has the most available resources.

- **Give preference to servers belonging to the selected group** (and, if the servers from that group are not available, use any available server).

Select a server group from the list. This option will attempt to process the object on the servers that are found within your server group. If the specified servers are not available, then the object will be processed on the next available server.

- **Only use servers belonging to the selected group**

This option ensures that BusinessObjects Enterprise will use only the specified servers that are found within the selected server group. If all of the servers in the server group are unavailable, then the object will not be processed.

Depending on the type of object, BusinessObjects Enterprise uses the following servers to process objects when you view them:

- Crystal reports run on the Crystal Reports Processing, Job and Cache Servers.
- Desktop Intelligence documents run on the Desktop Intelligence Processing, Job and Cache Servers.
- Web Intelligence documents run on the Web Intelligence Processing Server.

By selecting a particular server or server group, you can balance the load on your system by processing specific objects on specific job servers. You must first create server groups by using the "Servers" management area in the CMC, before you can select servers that belong to a selected group.

Note:

- If you choose the **Use the first available server** option, the Central Management Server (CMS) will check the job servers to see which one has the lowest load. The CMS does this by checking the percentage of the maximum load on each job server. If all of the job servers have the same load percentage, then the CMS will randomly pick a job server.
- You can also set the maximum number of jobs that a server will accept. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To specify default servers for processing an object

1. In the "Folders" management area of the CMC, select an object.
2. Click **Manage > Default Settings**.

Note:

You can specify default servers for a report object in two different places. If you want to specify the default servers used to schedule a report object, use **Manage > Default Settings > Scheduling Server Group**. If you want to specify the default servers used to process an object when you view it, use one of the options in step 3.

The "Default Settings" dialog box appears.

3. Choose one of these options from the navigation list:
 - If the object you selected is a Crystal report, click **Viewing Server Group**.
 - If the object you selected is a Web Intelligence document, click **Webi Process Settings**.
 - If the object you selected is a Desktop Intelligence document, click **Deski Process Settings**.
4. Choose the server option you want to use.
5. Click **Save & Close**.

Related Topics

- [Specifying default servers](#)

Changing database information

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

You can select your database type and set the default database logon information by using **Manage > Default Settings**. In the "Default Settings" dialog box, you can view the data source or data sources for your report object and its instances. You can also choose to prompt the user for a logon name and password when he or she views a report instance.

To change database settings

Note:

If you selected multiple report objects for which you want to change database settings, only those report objects that have the same data source connection will be updated.

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Manage > Default Settings**.

The "Default Settings" dialog box appears.

3. Click **Database Configuration** on the navigation list.
4. Select **Use original database logon information from the report** or **Use custom database logon information specified here**.

If you select the first option, you can specify a user name and password to be used with the original report database.

If you select the second option, you can specify a server name (or a DSN in the case of an ODBC data source), a database name, a user name, and a password for a number of predefined database drivers, or for a custom database driver that you've specified. If you've changed the default table prefix in your database, specify a custom table prefix here.

For a complete list of supported databases and drivers, refer to the `platform.txt` file included with your installation.

5. Select the database logon option you want.
 - **Prompt the user for database logon**

The system will prompt users for a password when they refresh a report.

Note:

This option has no effect on a scheduled instance. Also, BusinessObjects Enterprise only prompts users when they first refresh a report; that is, if they refresh the report a second time, they will not be prompted.

- **Use SSO context for database logon**

The system will use the user's security context, that is, the user's logon and password, to log on to the database.

Note:

For this option to work, you must have your system configured for end-to-end single sign-on, or for single sign-on to the database. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

- **Use same database logon as when report is run**

The system will use the same database logon information as was used when the report was run on the job server.

6. Click **Save & Close.**

Updating parameters

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

Parameter fields (with preset values) enable users to view and to specify the data that they want to see. If a report contains parameters, you can set the default parameter value for each field or fields (which is used whenever a report instance is generated). Through a BusinessObjects Enterprise application such as InfoView, your users are either able to use the report with the preset default value(s) or choose another value or values. If you do not specify a default value, users will have to choose a value when they schedule the report.

To update parameter settings

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Parameters** on the navigation list.

Note:

Parameters is available only if the report object contains parameters.

4. Under the "Value" column, click the value associated with the parameter you want to change.
Options appear that allow you to change the parameter value. Depending on the parameter value type, you either type a value in the field or choose a value from a list.
5. Click the **Clear Value** button if you want to clear the current value that is set for the specified parameter.
6. Select the **Prompt the user for new value(s) when viewing** check box if you want your users to be prompted when they view a report instance through a BusinessObjects Enterprise application such as InfoView.
7. Click **Save & Close**.

Updating prompts for Web Intelligence and Desktop Intelligence documents

Note:

This feature does not apply to Crystal reports objects. See [Updating parameters](#) instead.

Prompt fields (with preset values) enable users to view and to specify the data that they want to see. If a report contains parameters, you can set the default prompt value for each field or fields (which is used whenever a report instance is generated). Through a BusinessObjects Enterprise application such as InfoView, your users can either use the report with the preset default value(s) or choose another value(s). If you do not specify a default value, users will have to choose a value when they schedule the report.

To update the prompts for a Desktop Intelligence or Web Intelligence document

1. In the "Folders" management area of the CMC, select a Web Intelligence document.
2. Click **Manage > Default Settings**.

The "Default Settings" dialog box appears.

3. Click **Prompts** on the navigation list.

Note:

Prompts is available only if the Web Intelligence document object contains prompts.

4. Click **Modify**.

Options appear that let you select a prompt and values.

5. Select the prompt and enter a value for the prompt.

Tip:

If the available values are not displayed, click the **Refresh Values** button.

6. Repeat steps 5 and 6 for every prompt value you want to change.
7. Click **Apply**.
8. Click **Save & Close**.

Using filters

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects. Alternatively, you can use profiles to personalize views of the data.

You can set the default selection formulas for the report by using **Manage > Default Settings**. Selection formulas are similar to parameter fields in that they are used to filter results so that only the required information is displayed. Unlike parameters, end users will not be prompted for selection formula values when they view or refresh the report. When users schedule reports through a web-based client such as InfoView, they can choose to modify the selection formulas for the reports. By default, if any formulas are set in the CMC, they will be used by the web-based client. For more information on selection formulas, see the *Crystal Reports User's Guide*.

In addition to changing selection formulas, if you have developed your own processing extensions, you can select the processing extensions that you want to apply to your report.

When you use filters in conjunction with processing extensions, a subset of the processed data is returned. Selection formulas and processing extensions act as filters for the report.

Related Topics

- [How profiles work](#)
- [Applying processing extensions to reports](#)

To use filters

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Filters**.
4. Update or add new selection formulas.
 - **Record selection**
Use the **Record selection** field to create or edit a record selection formula or formulas that limit the records used when you or a user schedules a report.
 - **Group selection**
Use the **Group selection** field to create or edit a group selection formula or formulas that limit the groups used when you or a user schedules a report.
5. Click **Save & Close**.

Setting printer and page layout options

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

You can choose to print a report instance when scheduling it; report instances are always printed in Crystal Reports format. When printing a report, you can set the number of copies and the page range.

You can specify whether or not a report instance is printed, and if printed, the printer to use, the number of copies, and the page range. You can also

specify the custom layout settings for changing the page size and orientation (regardless of whether the report instance is printed or not).

Specifying a printer

You can choose to print a report (each time it runs) using the Crystal Reports Job Server's default printer or a different printer. BusinessObjects Enterprise prints your report after it is processed.

Note:

The Crystal Reports Job Server must run under an account that has sufficient privileges to access the printer you specify. See the "Managing and Configuring Servers" chapter for more information.

Specifying page layout

When viewing or scheduling a report instance to any format, you can specify page layout criteria such as page orientation, page size, and so on. The settings you choose affect how you'll see a report instance when displaying it.

Note:

Page layout settings are not specifically related only to scheduling a report to a printer, but also to the overall look of the report. The overall look is affected by the properties of the device for which the report is displayed in (that is, the font metrics and other layout settings of the display and/or the printer).

To assign a printer

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Print Settings** on the navigation list.
4. Select **Print Crystal report**.

The report is automatically sent to the printer in Crystal Reports format. This does not interfere with the format selected when scheduling the report.

5. Leave **Default printer** selected if you want to print to the Job Server's default printer; otherwise, select **Specify a printer**.

6. Enter a printer's path and name, select the number of copies, and choose the print page range.

If your job server is using Windows, in the **Specify a printer** field, type:

```
\\printserver\printername
```

Where *printserver* is the name of your printer server, and *printername* is the name of your printer.

If your job server is running on UNIX, in the **Specify a printer** field, type the print command that you normally use. For instance, type:

```
lp -d printername
```

Note:

Ensure that the printer you are using (on UNIX) is “shown” and not “hidden”.

7. Click **Save & Close**.

To set a report's print layout options

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Manage > Default Settings**.

The "Default Settings" dialog box appears.

3. Click **Print Settings** on the navigation list.
4. Select a default print mode.

- **Always print to PDF**

This option uses the PDF print mode settings when you print the report from a web viewer.

- **Follow Crystal Reports preference setting**

This option retains all the print mode settings that were made for the report in the CMC and allows SWF objects to print correctly.

5. On the "Set layout to" list, change your settings according to the type of layout you want. The options are as follows:

- **Report file default**

Choose this option if you want the page layout to conform to the settings that were chosen for the report in Crystal Reports.

- **Specify printer settings**

Choose this option if you want the page layout to conform to the settings of a specified printer. You can choose the Job Server's default printer or another printer.

When you choose this option, you can print scheduled report instances only to the printer you specify in the **Print when scheduling** area. In other words, you cannot set your report to display with one printer's setting and then print to a different printer.

- **Custom settings**

Choose this option if you want to customize all page layout settings. You can choose page orientation and page size.

6. Click **Save & Close.**

Related Topics

- [Setting printer and page layout options](#)

Processing extensions

BusinessObjects Enterprise offers you the ability to further secure your reporting environment through the use of customized processing extensions. A processing extension is a dynamically loaded library of code that applies business logic to particular BusinessObjects Enterprise view or schedule requests before they are processed by the system.

Note:

On Windows systems, dynamically loaded libraries are referred to as dynamic-link libraries (.dll file extension). On UNIX systems, dynamically loaded libraries are often referred to as shared libraries (.so file extension). You must include the file extension when you name your processing extensions.

Through its support for processing extensions, the BusinessObjects Enterprise administration SDK essentially exposes a “handle” that allows developers to intercept the request. Developers can then append selection formulas to the request before the report is processed.

A typical example is a report-processing extension that enforces row-level security. This type of security restricts data access by row within one or more database tables. The developer writes a dynamically loaded library that intercepts view or schedule requests for a report (before the requests are processed by the Crystal Reports Job Server, Crystal Reports Processing Server, or Report Application Server). The developer's code first determines the user who owns the processing job; then it looks up the user's data-access privileges in a third-party system. The code then generates and appends a record selection formula to the report in order to limit the data returned from the database. In this case, the processing extension serves as a way to incorporate customized row-level security into the BusinessObjects Enterprise environment.

Tip:

In BusinessObjects Enterprise XI, you can also set and enforce row-level security through the use of Business Views. For more information, see the *Business Views Administrator's Guide*.

The CMC provides methods for registering your processing extensions with BusinessObjects Enterprise and for applying processing extensions to particular object.

By enabling processing extensions, you configure the appropriate BusinessObjects Enterprise server components to dynamically load your processing extensions at runtime. Included in the SDK is a fully documented API that developers can use to write processing extensions. For more information, see the developer documentation available on your product CD.

In the current release, processing extensions can be applied only to Crystal report (.rpt) objects.

Related Topics

- [Applying processing extensions to reports](#)

Applying processing extensions to reports

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

BusinessObjects Enterprise supports the use of customized processing extensions. A processing extension is a dynamically loaded library of code

that applies your business logic to particular BusinessObjects Enterprise view or schedule requests before they are processed by the system. This section shows how to register your processing extension with BusinessObjects Enterprise, and how to apply an available processing extension to a particular report object.

Note:

On Windows systems, dynamically loaded libraries are referred to as dynamic-link libraries (.dll file extension). On UNIX systems, dynamically loaded libraries are often referred to as shared libraries (.so file extension). You must include the file extension when you name your processing extensions. Also, file names cannot include the \ or / characters.

Related Topics

- [Processing extensions](#)

Registering processing extensions with the system

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

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. The BusinessObjects Enterprise installation 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\Business Objects\BusinessObjects Enterprise 12.0\win32_x86\ProcessExt`. On UNIX, it is the `bobje/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 a Crystal Reports 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 a Crystal Reports Job Server, Crystal Reports Processing Server, or RAS.

Note:

If the processing extension is required only for schedule/view requests made to a particular server group, you need only copy the library onto each processing server in the group.

Related Topics

- [Sharing processing extensions between multiple servers](#)

To register a processing extension with the system

1. Go to the "Applications" management area of the CMC.
2. Select **CMC**.
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 the CMC.

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

Related Topics

- *To select a processing extension for a report*

To select a processing extension for a report

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

1. Go to the "Folders" management area of the CMC.
2. Select the report object that you want to apply your processing extension to.
3. On the **Manage** menu, click **Default Settings**.
The "Default Settings" dialog box appears.
4. Click **Extensions** on the navigation list.
5. Select your processing extension from the **Available processing extensions** list, and click > to move it to the **Use these processing extensions (in the order listed)** list.

Note:

Your processing extensions appear in this list only after you have registered them with the system. For details, see *Registering processing extensions with the system*.

Tip:

You may apply more than one processing extension to a report object. Repeat this step for each processing extension; then use the **Move Up** and **Move Down** buttons to specify the order in which the processing extensions should be used.

6. Click **Save & Close**.

Your processing extension is now enabled for this report object.

Sharing processing extensions between multiple servers

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

If you want to put all processing extensions in a single location, you can override the default processing extensions directory for each Crystal Reports Job Server, Crystal Reports Processing Server, and RAS. First, copy your processing extensions to a shared directory on a network drive that is accessible to all of the servers. Map (or mount) the network drive from each server's machine.

Note:

Mapped drives on Windows are valid only until you reboot the machine. For details, see the Troubleshooting Chapter of the *SAP BusinessObjects Enterprise Administrator's Guide*.

If you are running servers on both Windows and on UNIX, you must copy a .dll and an .so version of every processing extension into the shared directory. In addition, the shared network drive must be visible to Windows and to UNIX machines (through Samba or some other file-sharing system).

Finally, change each server's command line to modify the default processing extensions directory. Do this by adding `-report_ProcessExtPath absolute path` to the command line. Replace *absolute path* with the path to the new folder, using whichever path convention is appropriate for the operating system that the server is running on (for example, `M:\code\extensions`, `/home/shared/code/extensions`, and so on).

To modify the default processing extensions directory, use the CMC to stop the server. Then open the server's Properties to modify the command line. Start the server again when you have finished.

Working with hyperlinked reports

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

Crystal Reports lets you use hyperlinks to navigate from one report object to another. You can move to a Report Part within the report itself, to other report objects or their parts, or to specific instances of reports or Report Parts. This navigation is available only in the new script-based DHTML viewers (zero-client, server-side viewers) included in BusinessObjects Enterprise XI and above. By linking directly from one object to another, the required data context is passed automatically so that you navigate to the object and data that is relevant.

Initially, when you add hyperlinks between reports in Crystal Reports, you create a link from one file directly to another. However, when you add linked report files simultaneously to the same object package, the links are modified to point to managed report objects. (Each link is changed, so that it references the appropriate destination report by Enterprise ID, rather than by file path.) Also, the modified links become relative inside the object package. When you schedule the object package, BusinessObjects Enterprise processes its reports, and again modifies hyperlinks within each report instance: hyperlinks between report objects in an object package are converted to hyperlinks between report instances in a specific instance of the object package.

To view hyperlinked reports, you must publish both the home and destination reports to the same BusinessObjects Enterprise system. (A home report is one that contains a hyperlink to another report: the destination report.)

Note:

For information about how to create hyperlinks between report objects, see the *Crystal Reports Online Help*.

Related Topics

- [Scheduling objects using object packages](#)

Adding reports with existing hyperlinks

The recommended method for creating hyperlinked reports is first to publish the individual reports, then create hyperlinks between them. However, this is not always possible.

To add hyperlinked reports to the repository, use the Publishing Wizard to add the reports (that are linked to each other) to the same object package. When you publish reports this way, the hyperlinks are converted to relative links.

Note:

- This feature does not apply to Desktop Intelligence and Web Intelligence document objects.
- If you add hyperlinked reports independently of each other, rather than adding them simultaneously to the same object package, all hyperlinks between the reports will break. You must re-establish the links using Crystal Reports and save the report back to BusinessObjects Enterprise. (For more information, see the *Crystal Reports Online Help*.)

Related Topics

- [To add reports to the repository and then hyperlink them](#)

Viewing hyperlinked reports

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

BusinessObjects Enterprise supports navigation between hyperlinked reports only with script-based viewers, specifically the DHTML and Advanced DHTML viewers in InfoView. To change your preferred viewing format in the CMC, click the **Preferences** link in the upper-right corner of the CMC, and select the appropriate viewing format. For information on how to change your preferred viewing format, see the *SAP BusinessObjects Enterprise InfoView User's Guide*.

Parameter information is not carried over between the home and destination reports. That is, when you view a destination report by clicking a hyperlink in a home report, you are prompted to enter any parameters that the destination report requires.

Security considerations

To view hyperlinked reports through BusinessObjects Enterprise, you must have the appropriate rights both in BusinessObjects Enterprise and at the database level.

In BusinessObjects Enterprise, to view a destination report through a hyperlink in a home report, you must have View rights to the destination report. When the hyperlink points to a report object, you must have View On Demand rights to be able to refresh the data against the data source.

Database logon information is carried over between hyperlinked reports. If the credentials you specified to view the home report are not valid for the destination report, you are prompted for a valid set of database logon credentials for the destination report.

Related Topics

- [Working with access levels](#)

To add reports to the repository and then hyperlink them

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

To avoid breaking hyperlinks between reports, it is best to publish the reports first and then to create the hyperlinks.

1. Create the reports, without hyperlinks, in Crystal Reports.
2. Add them to BusinessObjects Enterprise.
3. Use Crystal Reports to log on to your BusinessObjects Enterprise system.
4. Create the hyperlinks between the home and destination reports.

See the *Crystal Reports Online Help*.

Crystal Reports automatically determines what type of link—relative or absolute—to establish between the reports. In BusinessObjects Enterprise, relative links are those between reports in the same object package, and absolute links are links to specific report objects or instances.

To view the universes for a Web Intelligence document

You build queries for Web Intelligence documents using objects in a universe. A universe is a representation of the information available in the database. In the CMC, you can view which universes are used by a Web Intelligence document.

1. In the "Folders" management area of the CMC, select a Web Intelligence document object.
2. Click **Manage > Default Settings**.

The "Default Settings" dialog box appears.

3. Click **Report Universes** on the navigation list.

A list of the universes that are used by the document appears.

Program object management

This section explains program objects and instances, and how to manage them through the Central Management Console (CMC). Additionally, this section covers type-specific program object configuration, and security considerations for program objects.

What are program objects and instances?

A program object is an object in BusinessObjects Enterprise that represents an application. Adding a program object to BusinessObjects Enterprise allows you to use BusinessObjects Enterprise to schedule and run the program object and to manage user rights in relation to the program object.

When you add a program object or its associated files to BusinessObjects Enterprise, they are stored in the Input File Repository Server (FRS). Each time a BusinessObjects Enterprise program runs, the program and files are passed to the Program Job Server, and BusinessObjects Enterprise creates a program instance. Unlike report instances, which you can view in their completed format, program instances exist as records in the object history. BusinessObjects Enterprise stores the program's standard out and standard error in a text output file. This file appears when you click a program instance in the object History.

In order for a program object to be successfully scheduled and run, you must provide logon information for the account that the program object will run as.

Related Topics

- [Overview](#)

Program types

Three types of applications can be added to BusinessObjects Enterprise as program objects:

- Executable

Executable programs are binary files, batch files, or shell scripts. They generally have file extensions such as: .com, .exe, .bat, .sh. You can publish any executable program that can be run from the command line on the machine that runs the Program Job Server.

- Java

You can publish any Java program to BusinessObjects Enterprise as a Java program object. For Java program objects to have access to Java SDK objects, your class must implement the `IProgramBase` interface from the BusinessObjects Enterprise Java SDK (`com.businessobjects.sdk.plugin.desktop.program.IProgramBase`). For details, see the *SAP BusinessObjects Enterprise Java SDK Developer Guide*.

- Script

Script program objects are JScript and VBScript scripts. They are run on Windows using an embedded COM object and can—once published—reference the BusinessObjects Enterprise SDK objects. For details, see the *SAP BusinessObjects Enterprise .NET SDK Developer Guide*.

Note:

Script program objects are not supported on UNIX.

Note:

As the administrator, you can choose to enable or disable any of the types of program objects.

Once you have published a program object to BusinessObjects Enterprise, you can configure it in the "Folders" management area of the CMC. For each type of program object (Executable, Java, or Script) you can choose to specify command-line arguments and a working directory. For executable and Java programs, there are additional ways, both required and optional, to configure the program objects and provide them with access to other files.

Tip:

Program objects allow you to write, publish, and schedule scripts or Java programs that run against BusinessObjects Enterprise, and perform maintenance tasks, such as deleting instances from the history. Furthermore, you can design these scripts and Java programs to access BusinessObjects Enterprise session information. This ensures that the scheduled program objects retain the security rights or restrictions of the user who scheduled

the job. (Your scripts or java programs require access to the BusinessObjects Enterprise SDK. For details, see the *SAP BusinessObjects Enterprise .NET SDK Developer Guide* or the *SAP BusinessObjects Enterprise Java SDK Developer Guide*.)

Related Topics

- [Authentication and program objects](#)

Setting program processing options

To specify 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. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Program Parameters** on the navigation list.
4. In the **Arguments** field, type the command-line arguments for your program, using the same format you would use at the command line itself.

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**.

Setting a working directory for a program object

By default, when a program object runs, BusinessObjects Enterprise creates a temporary subdirectory in the Program Job Server's working directory, and uses this subdirectory as the working directory for the program. The subdirectory is automatically deleted when the program finishes running.

You can specify an alternative working directory for the program object with the **Default Settings** command on the **Manage** menu. Or, you can modify the default setting for the working directory for the Program Job Server.

Note:

The account under which the program runs must have appropriate rights to the folder that you set as the working directory. The level of file permissions required depend on what the program does; however, the program's account generally needs read, write, and execute permissions to the working directory.

Related Topics

- [Authentication and program objects](#)

To set a working directory for a program object

1. In the "Folders" management area of the CMC, select the program object.
2. Click **Manage > Default Settings**.

The "Default Settings" dialog box appears.

3. Click **Program Parameters** on the navigation list.
4. In the **Working Directory** field, type 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`, type `C:\working_directory`

On UNIX, type `/working_directory`

5. Click **Save & Close**.

To modify the default working directory for the Program Job Server

1. Go to the "Servers" management area of the CMC.
2. Select the Program Job Server.
3. Click **Manage > Properties**.
The "Properties" dialog box appears.
4. In the **Temporary Directory** field, type the full path to the directory you want to set as the working directory for the Program Job Server.
5. Click **Save & Close**.

Configuring executable programs

When you publish an executable program object to the CMC, you can:

- Configure the object to have access to external or auxiliary files.
- Customize environment variables for the shell in which BusinessObjects Enterprise runs the program.

Related Topics

- [Configuring Java programs](#)

To specify paths to required files

Some binary files, batch files, and shell scripts require access to external or auxiliary files to run. Aside from setting a working directory for the program object, there are two ways to provide access to these files:

- If a required file is on the same machine as the Program Job Server, you can specify the full path to the file.
- Alternatively, if the file is not located on the Program Job Server, you can upload the file to the File Repository Server, which will pass the files to the Program Job Server as necessary.

1. In the "Folders" management area of the CMC, select the executable program object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Program Parameters** on the navigation list.
4. In the **External Dependencies** field, type the full path to the required file and click **Add**.
5. Repeat step 4 for each file required.
6. Click **Save & Close**.

Tip:

To edit or remove external dependencies that you have specified, select the file path (in the list of external dependencies in the Program Parameters section) and click the appropriate button, either **Edit** or **Remove**.

To upload required files

1. In the "Folders" management area of the CMC, double-click the link for the executable program object.

The "Properties" dialog box appears.

2. Click **Associated Files** on the navigation list.
3. Click **Browse** to navigate to the required file, then click **Add File**.
4. Repeat step 3 for each required file.
5. Click **Save & Close**.

Tip:

To remove auxiliary files that you have specified, select the file(s) from the **Current auxiliary files** list and click **Remove File(s)**.

To add an environment variable

In the CMC, you can configure your program by adding or modifying environment variables. Modifications to an existing environment variable override this variable, rather than append to it. Any changes you make to environment variables exist only in the temporary shell in which BusinessObjects Enterprise runs the program. Thus, when the program exits, the environment variables are destroyed.

1. In the "Folders" management area of the CMC, click the program object.
2. Click **Manage > Default Settings**.

The "Default Settings" dialog box appears.

3. Click **Program Parameters**.
4. In the **Environment Variables** field, type the environment variables you want to set, and then click **Add**.

Use the form `name=value`, where `name` is the environment variable name and `value` is the value for the environment variable. For example, you can set the path variable to append a user's bin directory to the existing path:

- On Windows, you might type: `path=%path%;c:\usr\bin`
- On UNIX, you might type: `PATH=$PATH:/usr/bin`

Note:

BusinessObjects Enterprise 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 typed in upper case.

5. Click **Save & Close**.

Tip:

To edit or remove environment variables that you have specified, select the variable from the **Environment Variables** list, and click the appropriate button, either **Edit** or **Remove**.

Configuring Java programs

To successfully schedule and run Java programs in BusinessObjects Enterprise, you must specify the required parameters for the program object.

Additionally, you can provide the Java program with access to other files located on the Program Job Servers, and you can specify Java Virtual Machine options.

To specify default parameters for scheduling Java programs

To successfully schedule and run a Java program, you must set certain parameters in the CMC, including the base name of the .class file that implements the IProgramBase interface from the BusinessObjects Enterprise Java SDK.

Note:

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

1. In the "Folders" management area of the CMC, select the Java program object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Program Parameters** on the navigation list.
4. In the **Class to run** field, type the base name of the .class file that implements the IProgramBase from the BusinessObjects Enterprise Java SDK (`com.businessobjects.sdk.plugin.desktop.program.IProgramBase`).
For example, if the file name is `Arius.class`, type `Arius`.

5. Click **Save & Close**.

These default values are used when scheduling a Java program. The parameter values can be also modified before running a scheduling job under the **Schedule > Program Parameters** menu.

Note:

If your scheduled job fails to run due to an `OutOfMemoryError` error, increase the maximum heap size allocated to the JVM. JVM arguments can be set in the **JVM arguments** field in the "Program Parameters" section. Specify a maximum heap size that is suitable for your Java program to run, for example: `-Xmx1024m`. The **JVM arguments** field should only be used to resolve errors and should be left blank otherwise.

To provide Java programs with access to other files

You can provide Java programs with access to files, such as Java libraries, located on the Program Job Server.

1. In the "Folders" management area of the CMC, select the Java program object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Program Parameters** on the navigation list.
4. In the **Classpath** field, type the full paths to the locations of any Java library files that are required by the Java program, and stored on the Program Job Server.

You must separate multiple paths with the classpath separator that is appropriate to your operating system: a semi-colon for Windows, a colon for UNIX.

5. Click **Save & Close**.

Authentication and program objects

Be aware of the potential security risks associated with the publication of program objects. As the administrator, you must protect the system against abuse. 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.

You can control the types of program objects users can run, and you can configure the credentials required to run program objects.

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, the administrator, to set up a specific user account for the program, and assign it appropriate rights, to have the program object run as that account.

Alternatively, users who add program objects to BusinessObjects Enterprise can assign their own credentials to a program object, to 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

BusinessObjects Enterprise allows you to set security for all program objects. For Java programs, BusinessObjects Enterprise forces 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 BusinessObjects Enterprise Java SDK and allows program objects full rights to all 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.
- By default, the Java Policy File is installed to the Java SDK directory in the BusinessObjects Enterprise install root directory. For example, a typical location on Windows is: C:\Program Files\Business Objects\BusinessObjects Enterprise 12.0\conf\crystal-program.policy
- On UNIX, a typical location is .../solaris_install/bobje/enterprise12/JavaSDK/crystal-program.policy

To enable or disable a type of program object

1. In the "Applications" area, select **CMC**.
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 BusinessObjects Enterprise.

4. Click **Save & Close**.

To specify a user account for a program object

1. In the "Folders" management area of the CMC, select the program object.
2. Click **Manage > Default Settings**.
The "Default Settings" dialog box appears.
3. Click **Program Logon** on the navigation list.
4. In the **User Name** and **Password** fields, type the credentials for the user account under which the program should run.
5. Click **Save & Close**.

Object package management

This section explains object packages and instances, and how to manage them through the Central Management Console (CMC). Additionally, this section explains how to create an object package and how to add objects to an object package.

What are object packages, components, and instances?

Object packages function as distinct objects in BusinessObjects Enterprise. Think of them as folders you can schedule, along with all of their contents.

Object packages can be composed of any combination of report and program objects that are published to the BusinessObjects Enterprise system. (Non-BusinessObjects Enterprise objects, such as Excel, Word, Acrobat, Text, Rich Text, PowerPoint, and Hyperlink objects, cannot be added to object packages.)

Placing multiple objects in a single object package allows you to schedule them simultaneously. For reports, object packages allow users to view synchronized data across reports. Component objects are not autonomous. They have more limited configuration options than other objects, and they do not appear in the list of all objects in the "Folders" management area of the CMC. Rather, you can only view them by opening their object package.

BusinessObjects Enterprise creates an object package instance each time it runs an object package. The object package instance contains individual instances of each of its component objects. Component instances are tied to object package instances, rather than to component objects. For example, if you run an object package, and thereby create an instance, then remove a report object from the object package, the existing object package instance does not change; it still contains the report instance from the report object that you removed. Future instances of the object package, however, will reflect the change.

For hyperlinked report instances in object package instances, the hyperlinks point to the other report instances in the same object package instance.

Related Topics

- [Working with hyperlinked reports](#)

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. In the **Title** field, type the name of the object package you want to create.
4. In the **Description** field, type a description of the object package.
This field is optional.
5. Click **OK**.

Note:

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** on the menu.

Adding objects to an object package

In the CMC, after you have created an object package, you can add report and/or program component objects to it. You can add previously unpublished objects directly to the object package, or you can copy existing objects into the object package. You can only move copies of existing objects into the object package, or between object packages; you cannot move the existing objects themselves.

When you copy an object into an object package, the component object retains the same settings as the original object. However, once you create the copy of the original object inside the object package, the component and the original are separate entities. Changes in one object are not reflected in the other.

Note:

You can also add objects to new or existing object packages using the Publishing Wizard.

Related Topics

- [To copy an object](#)
- [Publishing Wizard procedures](#)

To add a new object directly 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 > Crystal Report** or **Program File** depending on the object you want to add.
Different dialog boxes appear depending on the option you selected.
3. In the **Filename** field, enter the name of the file, or click **Browse** to navigate to the object you want to publish.
4. Set the appropriate properties.
 - For reports, specify whether you want to keep saved data.
 - For programs, set the program type: Executable, Java, or Script.
5. Click **OK**.

Configuring object packages and their objects

Object packages are intended to save you time scheduling objects that have similar scheduling requirements. As a result, you configure some parameters at the object package level, and some at the object level, that is, for the individual objects in the object package.

For example, you have to specify the destination for an object package, but you cannot specify destinations for the individual objects in the package. When the system runs the object package, it will save the output instances to the destination you specified for the object package.

Note:

Because the objects in an object package are copies of objects that exist outside the package, the changes you make will not affect the objects outside the object package.

Authentication and object packages

Object packages simplify both Enterprise and database authentication. You enter your Enterprise authentication only once to schedule the object package, including all of its component objects. Consequently, you must have Schedule rights for each of the objects inside the object package. If you attempt to schedule a package that contains one or more component objects to which you do not have schedule rights, the component instance(s) fail(s).

For database authentication, you specify database logon information for each report component object in the object package. (If you copied the report into the object package, it initially inherits the database logon information of the original report.)



Scheduling Objects

23

chapter



Overview

This section provides information on scheduling objects. It provides detailed instructions for scheduling objects individually and in batches, and scheduling with events. It also describes distributing objects, specifying schedule notifications, and managing instances.

Scheduling

Scheduling is a process which allows you to run an object automatically at specified times. When you schedule an object, you choose the recurrence pattern that you want and specify additional parameters to control exactly when and how often the object will be run.

At the time you schedule an object, the system creates a scheduled instance. Although a scheduled instance appears in the "History" dialog box of a respective object (with a status of Recurring or Pending), it contains solely object and schedule information—it does not contain any data.

When the system runs the object, it creates an output instance for the object (for example, a report or program instance). A report instance contains actual data from the database. A program instance is a text file that contains the standard output and standard error produced when the program object was run. Output instances also appear in the "History" dialog box of an object and have a status of Success or Failed.

For end users to schedule and run objects, they must use a web-based client such as InfoView or a custom web application. InfoView is designed primarily to schedule objects and view reports, whereas the CMC enables you to manage and administer objects in addition to scheduling objects and viewing reports.

About the recurrence options and parameters

When you schedule an object, you choose the recurrence pattern that you want. For example, you select **Daily** or **Weekly**, and then the run option (for example, indicating the days of the week on which you want the object to run). You then specify additional parameters to control exactly when and how often the object will be run.

Which run options and parameters are available depends on the recurrence pattern you selected. In many cases the same parameters appear, such as start and end dates.

Related Topics

- [Recurrence patterns](#)
- [Run options and parameters](#)

Recurrence patterns

When scheduling an object, you can choose from the recurrence patterns summarized by the following table.

Table 23-1: Recurrence patterns

Recurrence pattern	Description
Now	The object will be run as soon as the user clicks Schedule .
Once	The object will be run only once. It can be run now or in the future, or when a specified event has occurred.
Hourly	The object will be run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The object will be run every day. It can be run once or several times a day. You can specify at what time it will run, as well as a start and end date.

Recurrence pattern	Description
Weekly	The object will be 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 object will be run every month or every several months. You can specify on which days of the month and at what time it will run, as well as a start and end date.
Day of Month	The object will be run on a certain day of every month. You can specify the day it will run, as well as a start and end date.
First Monday of Month	The object will be run on the first Monday of every month. You can specify a start and end date.
Last Day of Month	The object will be run on the last day of every month. You can specify a start and end date.
Day of Week of Month	The object will be run on a particular day of a particular week every month. You can specify the day and the week, as well as the start and end date.
Calendar	The object will be run on the dates specified in a calendar that has previously been created.

Related Topics

- [Calendars overview](#)

Run options and parameters

This section describes the Run parameters for scheduling an object. Not all parameters apply in all cases, but when they apply, their function is the same.

Table 23-2: Run options

Run option	Description
X and N variables	<p>Applies to certain Daily and Monthly recurrence patterns only. When you select a Run option that contains these variables, the system displays their default values. You can then change these values as needed.</p> <p>For example, if you select the Daily recurrence pattern and the Every N hour(s) and X minute(s) Run option, you could specify to run the report every 4 (X) hours and 30 (N) minutes. If you don't change the X or N value, the system will run the report every hour.</p>
Run Days	<p>These options appear if you select the Weekly recurrence pattern. You can choose the days of the week on which you want your job to run by deleting the checkboxes of the appropriate days.</p>

Run option	Description
Start Time	<p>Applies to most, but not all recurrence patterns and Run options. The default is the current date and time. The system will run the object according to the schedule that you specified, as soon as it can, after the Start Time has passed.</p> <p>For example, if you specify a start time that is three months into the future, the system won't run the object until the start date has passed, even if all the other criteria are met. After that, the system will run the report at the specified time.</p>
End Time	<p>Applies to most, but not all, recurrence patterns and Run options. The default is the current time and a date in the distant future, to ensure an object will be run indefinitely. Specify a different End Time if required. Once the End Time has passed, the system no longer runs the object.</p>
Number of retries allowed	<p>Always applies. The number of times the system attempts to process an object if the first attempt is not successful. By default, the number is zero.</p>

Run option	Description
Retry interval in seconds	Always applies. The period, in seconds, that the system will wait before it attempts to process the object again if the first attempt is unsuccessful.

To schedule an object

1. In the "Folders" management area of the CMC, select an object.

Note:

To change the default schedule settings for the object, click **Default Settings** when you open the "Schedule" dialog box. Set the scheduling settings and click **Save**.

2. Click **Actions > Schedule**.

The "Schedule" dialog box appears, showing the default settings for the object.

3. Enter an appropriate instance title.
4. Click **Recurrence** and select the recurrence pattern you want.
For example, select **Weekly**.

5. Specify the Run option and parameters that you want.

For example, select **Weekly** and then specify Monday, Wednesday, and Friday.

6. Set any of the other schedule options and parameters as required.
7. Click **Schedule**.

The system will create a scheduled instance and run it according to the schedule information you specified. You can view the scheduled instance on the "History" page for the object.

Related Topics

- [Recurrence patterns](#)
- [Run options and parameters](#)
- [Setting general scheduling options](#)
- [Managing and viewing the history of instances](#)

Scheduling objects using object packages

You can schedule objects in batches using the object packages feature. Object packages are distinct objects in BusinessObjects Enterprise. They can contain any combination of objects that can be scheduled, such as reports, program objects, and Web Intelligence documents. Using object packages simplifies authentication, and allows users to view synchronized data across instances for different objects.

To schedule objects using object packages, first create an object package. Then copy existing objects into the object package. Finally, schedule the object package as you would any object. Alternatively, you can add objects to an object package using the Import Wizard.

Note:

You must configure the processing information of each of the components of an object package individually. For example, if you want a report object in an object package to print when scheduled, you must configure it by clicking **Components** in the "Schedule" dialog box and clicking the title of the component you wish to print. You can then expand **Print Settings** for the component and set it to print as you would when scheduling the component on its own.

Related Topics

- [Object package management](#)
- [Configuring object packages and their objects](#)
- [Working with hyperlinked reports](#)

Scheduling an object with events

When you schedule an object with events, the object is run only when the additional condition (that is, the event) occurs. You can schedule objects to wait for any or all of the three event types: file-based, custom, and schedule-based. If you want a scheduled object to trigger an event, you must choose a schedule-based event.

Note:

A file-based event is triggered upon the existence of a specified file. A custom event is triggered manually. A schedule-based event is triggered by another object being run.

Scheduling objects based on an event

When you schedule an object that waits for a specified event, the object will run only when the event is triggered, and only when the rest of the schedule conditions are met. If the event is triggered before the start date of the object, the object will not run. If you have specified an end date for this object, and if the event is not triggered before the end date occurs, the object will not run because not all of the conditions will have been met. Also, if you choose a weekly, monthly, or calendar schedule, the object will have a specified time frame in which it can be processed. The event must be triggered within this specified time for the object to run. For example, if you schedule a weekly report object that runs every Tuesday, the event must be triggered before the end date of the instance (the end of Monday, in this example).

Scheduling objects to trigger an event

You can also schedule an object which triggers a schedule-based event upon completion of the object being run. When the object is run, BusinessObjects Enterprise will trigger the specified event. For a schedule-based event, if the event is based on the instance being run successfully, for example, the event won't be triggered if the instance fails.

Note:

To schedule an object with events, you must first ensure that you have created the event.

Related Topics

- [Managing events overview](#)

- *Schedule-based events*

To schedule an object to run based on events

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions** > **Schedule**.
3. From the **Run object** list on the left of the page, select a recurrence pattern: Once, Daily, Weekly, Monthly, or by Calendar.
4. Select a run option.
5. Select and complete the schedule parameters for your object (scheduling option, Start Date, End Date, and so on).
6. Click **Events**, select from the list of **Available Events**, and click > to add the event(s) to the list of **Events to wait for**.

Tip:

Click >> to add all the available events.

7. Click the **Schedule** button to schedule the object.

Related Topics

- *Recurrence patterns*
- *Run options and parameters*

To schedule an object to trigger an event

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions** > **Schedule**.
3. From the **Run object** list on the left of the page, select a recurrence pattern: Once, Daily, Weekly, Monthly, or by Calendar.
4. Select and complete the schedule parameters for your object (scheduling option, Start Date, End Date, and so on).
5. In the **Events** area, select from the list of **Available Schedule Events** and click > to add the events(s) to the list of **Events to trigger on completion**.

Note:

You can only select schedule-based events in this list.

Tip:

Click >> to add all the available events.

6. Click the **Schedule** button to schedule the object.

Related Topics

- [Recurrence patterns](#)

Setting general scheduling options

BusinessObjects Enterprise allows you to control the process and schedule settings for an object.

Related Topics

- [To schedule an object](#)
- [Setting notification for the success or failure of a scheduling job](#)
- [Specifying alert notification](#)
- [Selecting a destination](#)
- [Choosing a format](#)
- [Scheduling an object for a user or group](#)
- [Selecting cache options for Web Intelligence or Desktop Intelligence documents](#)

Setting notification for the success or failure of a scheduling job

You can set scheduling options that automatically send notification when an object instance succeeds or fails. You can send notification using audit or email notification. You can also combine multiple notification methods, and provide different notification settings for successful and failed instances.

For example, you may have a large number of reports that run every day. You need to check each instance to make sure it ran properly, and then send out emails to the users who need to know that the new report is available. With thousands of reports, it would take too much time to manually check the reports and contact the users who need the information. Using notification settings in BusinessObjects Enterprise, you can set each object to notify you

automatically when the report fails to run properly, and you can automatically inform users when new report instances run successfully.

Determining the success or failure of a scheduling job

When you schedule an object, the scheduled instance either succeeds or fails. The conditions required for an instance's success or failure depend on the type of object you schedule:

- Report objects, Desktop Intelligence document objects, and Web Intelligence document objects

A report instance or document object instance runs successfully if it doesn't encounter any errors while processing the object or accessing the database. An instance may fail if the user does not provide the correct parameters or logon information.

- Program objects

For program objects, the program must run in order to succeed. If the program does not run, the instance is considered a failure. If the program runs, but does not perform the tasks it is supposed to, it is still considered a successful instance because the program object ran. BusinessObjects Enterprise does not monitor problems with the program object's code.

- Object packages

An object package may fail if one of its components fails. To change this setting, open the object package's **Default Settings** from its Properties, click **Component Failure**, and clear the **Scheduled package fails upon individual component failure** option.

You can also set scheduling options for individual objects within an object package. You can do this by choosing the component you want to set options for in the **Components** section of the "Scheduling" dialog box. You can then set the component's notification, database logon, filters, format, print, parameters, server groups, and alert settings as applicable to the component.

Note:

You cannot set audit or email notification for object packages, but you can set any type of notification for the individual objects in the object package. You can also schedule object packages with events.

Related Topics

- [Schedule-based events](#)

About notification

You can set notification at the object level. You can select unique notification options for each object, sending different types of notification for different conditions. For object packages, you can set only event notification, which will trigger an event based on success or failure of the object package. To monitor object successes and failures from a more general perspective, use the auditing functionality within BusinessObjects Enterprise.

If notification fails, then the object instance fails. For example, if an email notification sends a message to an invalid email address, then the notification fails and the object instance is recorded as a failure in the object's history.

You can choose to notify using:

- **Audit notification**

To use audit notification, you must configure the auditing database and enable auditing for the servers. If you use auditing to monitor your BusinessObjects Enterprise system, you can use audit notification. For more information about configuring the auditing database and enabling auditing, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

When you select audit notification, information about the scheduled object is written to the auditing database. You can choose to have a notification sent to the auditing database when the job runs successfully, when it fails to run, or both.

- **Email notification**

You can send an email as a notification of an object instance's success or failure. You can choose the sender and recipients of the email message. You can send an email when the instance fails and when it succeeds. For example, you could send your administrator an email if the report fails, but when the report succeeds you can automatically send a notification to everyone who needs the report to let them know it is now available.

Note:

To enable email notification, you must have the Email SMTP destination enabled and configured on the job servers. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Note:

Notification of a scheduled object's success or failure is not the same as alert notification. Alert notification must be built into the design of the report. For example, alert notification can send an email to you whenever a specific value in the report exceeds \$1,000,000. In this case, the notification has nothing to do with the contents of the report — it's just about whether or not the report object instance has failed or succeeded.

To set notification for an instance's success or failure

1. Select an object in the "Folders" management area of the CMC.
2. Click **Actions > Schedule**.
3. On the navigation list, expand **Notification**.
4. Click the notification type (or types) you want to use.

Note:

If the notification type is already being used, it will be labeled "Enabled". If not, it will be labeled "Not in use".

5. Choose specific settings for the notification and click **Update**.

Table 23-3: Notification types

Notification type	Instruction
Audit	<ul style="list-style-type: none"> • To send a record to the auditing database when the job succeeds, select A job has been run successfully. • To send a record when the job fails, select A job has failed to run.

Notification type	Instruction
Email	<ul style="list-style-type: none">Choose whether you want to send a notification when the job fails or when it succeeds.To specify the contents and recipients of the email notification, expand the notification option(s) you have enabled, select Set the values to be used here, and provide the From and To email addresses, the email subject line, and the message. <p>Note: Separate multiple addresses or distribution lists by using semicolons.</p>

Note:

By default, the notification is sent to the server's default email destination. For details on how to change the default email settings, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Specifying alert notification

Note:

This feature does not apply to Desktop Intelligence and Web Intelligence document objects.

Alerts are custom messages, created in Crystal Reports, that appear when certain conditions are met by data in a report. Alerts may indicate actions to be taken by the user or information about report data. If the alert condition (as defined in Crystal Reports) is true, the alert is triggered and its message is displayed.

In BusinessObjects Enterprise, you can choose to send alert notification when scheduling a report. If you enable alert notification, messages are sent

through an SMTP server. You can configure email delivery options, specify the **To**, **Cc**, and **From** fields for the email, add subject and message information, set a URL for the viewer you want the email recipient to use, and set the maximum number of alert records to send.

Note:

- The Alert Notification link is available only if the report object contains alerts.
- Alerts are triggered in the report object even if you disable alert notification.
- To enable alert notification, you must have the Email SMTP destination enabled and configured on the job servers. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To set alert notification

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Actions > Schedule**.
3. On the navigation list, click **Alert Notification**.
4. Select the **Enable alert notification** check box if you want to send an alert notification.
5. Select either **Use default settings** or **Custom settings**.

If you select the first option, BusinessObjects Enterprise will deliver the alert notification using the Job Server's default settings. You can change these settings in the "Servers" management area. For more information, see the *SAP BusinessObjects Enterprise Web Application Deployment Guide*.

If you select the second option, you can specify the email settings in the software.

6. Type the URL for the viewer in which you want the email recipient to view the report. Alternatively, you can select the default viewer by clicking **Use default**.

The viewer URL appears in the hyperlink that is sent in the alert notification email. You can set the default URL by selecting the CMC application in the "Applications" management area of the CMC and clicking **Manage** and **Properties**. For more information, see the developer documentation available on your product CD.

Note:

You must use World Wide Web Consortium (W3C) URL encoding when typing the viewer URL. For example, replace spaces in the path with %20. For more information, see <http://www.w3.org/>

7. Type the maximum number of alert records to be included in the alert notification.

The hyperlink in the alert notification displays a report page that contains the records that triggered the alert. Use this field to limit the number of records displayed.

Tip:

The **Alert Name** and **Status** fields are set in Crystal Reports.

8. When you have finished setting all your scheduling options, click **Schedule**.

Selecting a destination

Using BusinessObjects Enterprise, you can configure an object or instance for output to a destination other than the default Output File Repository Server (FRS). When the system runs an object, it always stores the output instance on the Output FRS. Being able to choose an additional destination gives you the flexibility to deliver instances across your enterprise system or to destinations outside your enterprise system.

For example, you can set an object to have its output automatically delivered by email to other users.

Note:

You can also configure object instances to be printed after they have been run.

When you specify a destination other than “Default”, BusinessObjects Enterprise generates a unique name for the output file or files. To generate a file name, you can use a combination of ID, name or title of the object, owner information, or the date and time information. The available destinations are file locations, FTP, email, and BusinessObjects Enterprise inboxes.

The following destinations are available:

- Default destination location
- File Location
- FTP Location
- Email
- Inbox

Note:

You can change the destination setting for an object or instance either in the CMC or in InfoView. When you specify the destination settings through the CMC, these settings are also reflected in the default scheduling settings for InfoView.

Related Topics

- [Setting printer and page layout options](#)
- [Default destination support](#)
- [Unmanaged Disk destination support](#)
- [FTP support](#)
- [Email \(SMTP\) support](#)
- [Inbox support](#)

Default destination support

By default, object instances are saved to the Output File Repository Server (FRS). If you want to save instances to the FRS only and not to any other destinations, select that option.

To set your destination to default

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions** > **Schedule** and access the "Destination" page.
 - If you are scheduling a Crystal report or object package, click **Destination**.
 - If you are scheduling a Desktop Intelligence document, click **Format and destination**.
 - If you are scheduling a Web Intelligence document, click **Formats and Destinations**.
3. Ensure that **Default Enterprise Location** is set as the destination.

- If you are scheduling a Crystal report or object package, select **Default Enterprise Location** from the **Destination** list.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, ensure that no checkboxes are selected under "Output Format Details".
4. Set the rest of your scheduling options and click **Schedule**.

Unmanaged Disk destination support

When scheduling objects, you can configure the objects for output to an unmanaged disk. In that case, the system will save an output instance to both the Output File Repository Server and the specified destination.

If the object is a Web Intelligence document or an object package, you cannot specify Unmanaged Disk as a destination. However, for an object package you can configure the individual objects in the object package for output to Unmanaged Disk.

Note:

- To use a destination, you must have the destination enabled and configured on the job servers. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.
- The location must be a local directory on the processing server. For servers using Windows, the location can either be a Universal Naming Convention (UNC) path or a local directory.
- The processing server must have sufficient rights to the specified location.

To set your destination to file location

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions > Schedule** and access the "Destination" page.
 - If you are scheduling a Crystal report or object package, click **Destination**.
 - If you are scheduling a Desktop Intelligence document, click **Formats and destination**.
 - If you are scheduling a Web Intelligence document, click **Formats and Destinations**.
3. Select **File location** as the destination.

- If you are scheduling a Crystal report or object package, select **File Location** from the **Destination** list.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select **File Location** under "Output Format Details" and then click **Destination Options and Settings**.
4. If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect **Use the Job Server's defaults**.

Note:

You can change the default Job Server settings in the "Servers" management area of the CMC. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

"File location properties for scheduled objects" summarizes the file name properties and user information you can set to be used at schedule time.

Note:

You can specify a user name and password only for servers using Windows.

5. Choose whether to enable instance cleanup.
- If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect the **Clean up instance after scheduling** option.
 - If you are scheduling another type of object, select or deselect **Keep an instance in the history**.

When that option is selected, the system automatically deletes the report or program instance from the Output File Repository Server to keep the number of instances on the server to a minimum.

Note:

These instances are needed for auditing the event, so this setting is overruled if auditing is activated for the scheduled object.

6. Set other scheduling options as needed.
7. Click **Schedule**.

Table 23-4: File location properties for scheduled objects

Property	Description
Destination directory	Type a local location, mapped location, or a UNC path. If you are scheduling a Web Intelligence or Desktop Intelligence document and would like to create folders based on variables such as the Title of the instance, the owner, date and time, or users names, you can insert a variable by selecting it from the list. The variable is inserted at the end of the text in the text box.
File Name	<p>To let BusinessObjects Enterprise generate a file name, select Automatically generated.</p> <p>To choose a file name, select Specific name and enter the name you wish to use. If you are scheduling a Web Intelligence or Desktop Intelligence document, you can include the same variables in the file name as you could in the destination directory. If you would like to add the file extension to your indicated file name, ensure that Add file extension is selected.</p>
User Name	Specify a user who has permission to write files to the destination directory.
Password	Type the password for the user.

FTP support

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.

Note:

To use a destination, you must have the destination enabled and configured on the job servers. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To set an FTP server as the destination

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions > Schedule**, and access the "Destination" page.
 - If you are scheduling a Crystal report or object package, click **Destination**.
 - If you are scheduling a Desktop Intelligence document, click **Formats and destination**.
 - If you are scheduling a Web Intelligence document, click **Formats and Destinations**.
3. Select **FTP Server** as the destination.
 - If you are scheduling a Crystal report or object package, select **FTP Server** from the **Destination** list.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select **FTP Server** under "Output Format Details" and then click **Destination Options and Settings**.
4. If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect **Use the Job Server's defaults**.

If you select this option, BusinessObjects Enterprise will schedule an object using the Job Server's default settings. You can change these settings in the "Servers" management area. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

If you deselect this option, you can set the FTP and file name properties:

- **Host**

Enter the FTP host information.

- **Port**

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

- **User Name**

Specify a user who has the necessary rights to upload an object 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. To add a variable, choose a placeholder for a variable property from the list.

- **File Name**

To let BusinessObjects Enterprise generate a random file name, select **Automatically generated**. To enter a file name, select **Specific name**. You can also add a variable to the file name by choosing a placeholder for a variable property from the list. If you would like to include the file extension, ensure that you select **Add file extension**.

5. Choose whether to enable instance cleanup.

- If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect the **Clean up instance after scheduling** option.
- If you are scheduling another type of object, select or deselect **Keep an instance in the history**.

When that option is selected, the system automatically deletes the report or program instance from the Output File Repository Server to keep the number of instances on the server to a minimum.

6. Set your other scheduling options and click **Schedule**.

Email (SMTP) support

With Simple Mail Transfer Protocol (SMTP) mail support, you can choose to send the instances of an object, for example, a report instance, to one or more email destinations. After it has run the object, the system will send a copy of the output instance as an attachment to the email addresses you specified.

When you select the Email (SMTP) destination, the system will save the instance to the Output File Repository Server as well as email it to the specified destinations. BusinessObjects Enterprise supports Multipurpose Internet Mail Extensions (MIME) encoding.

Note:

To use a destination, you must have the destination enabled and configured on the job servers. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To schedule an object to an email destination

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions** > **Schedule** and access the "Destination" page.
 - If you are scheduling a Crystal report or object package, click **Destination**.
 - If you are scheduling a Desktop Intelligence document, click **Formats and destination**.
 - If you are scheduling a Web Intelligence document, click **Formats and Destinations**.
3. Select **Email Recipients** as the destination.
 - If you are scheduling a Crystal report or object package, select **Email Recipients** from the **Destination** list.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select **Email Recipients** under "Output Format Details" and then click **Destination Options and Settings**.

4. If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect **Use the Job Server's defaults**.

If you select this option, BusinessObjects Enterprise will schedule an object using the Job Server's default settings. You can change these settings in the "Servers" management area. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

If you deselect this option, you can specify the email settings and the file name properties.

Table 23-5: Email settings for scheduled objects

Field	Instruction
From	Type a return address.
To	Type an address to which you want the object to be sent. If you want to send the object to multiple addresses, use semicolons to separate them.
Cc	Type an address to which you want to send a copy of the object. If you want to send the object to multiple addresses, use semicolons to separate them.
Subject	Complete the Subject field. You can choose variables to include in the Subject field by choosing them from the list beside the text box.

Field	Instruction
Message	Type a short message, if required. You can choose variables to include in the message by choosing them from the list beside the text box.
Attach object instance to email message	Select this check box if you want a copy of the instance attached to the email.
Default File Name (randomly generated)	Select this option if you want BusinessObjects Enterprise to generate a random file name.
Specified File Name	Select this option if you want to enter a file name. You can choose variables to include in the Specified File Name field by choosing them from the list beside the text box. If you would like to add the file extension, ensure that Add file extension is selected.

5. Choose whether to enable instance cleanup.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect the **Clean up instance after scheduling** option.
 - If you are scheduling another type of object, select or deselect **Keep an instance in the history**.

When that option is selected, the system automatically deletes the report or program instance from the Output File Repository Server to keep the number of instances on the server to a minimum.

6. Set your other scheduling options and click **Schedule**.

Inbox support

When scheduling objects, you can configure objects for output to the inboxes of users. In this case, the system will save the instance to both the Output File Repository Server and the inboxes you specified. Instead of sending the actual file to the inboxes, you can choose to send a shortcut.

Note:

To use a destination, you must have the destination enabled and configured on the job servers. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

To schedule an object to an inbox destination

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions** > **Schedule** and access the "Destination" page.
 - If you are scheduling a Crystal report or object package, click **Destination**.
 - If you are scheduling a Desktop Intelligence document, click **Formats and destination**.
 - If you are scheduling a Web Intelligence document, click **Formats and Destinations**.
3. Select **Inbox** as the destination.
 - If you are scheduling a Crystal report or object package, select **FTP Server** from the **Inbox** list.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select **Inbox** under "Output Format Details" and then click **Destination Options and Settings**.
4. Choose whether to enable instance cleanup.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect the **Clean up instance after scheduling** option.
 - If you are scheduling another type of object, select or deselect **Keep an instance in the history**.

When that option is selected, the system automatically deletes the report or program instance from the Output File Repository Server to keep the number of instances on the server to a minimum.

5. If you are scheduling a Desktop Intelligence or Web Intelligence document, select or deselect **Use the Job Server's defaults**.

If you select this option, BusinessObjects Enterprise will schedule an object using the Job Server's default settings. You can change these settings in the Servers management area. For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

6. If you did not select **Use the Job Server's defaults**, set the following parameters; otherwise, skip this step.
 - a. Navigate to and select the users or groups from the "Available Recipients" panel and click > to add them to the **Selected Recipients**.

Tip:

You can click >> to add all the available recipients, and < or << to remove the selected or all recipients.

- b. To let BusinessObjects Enterprise to generate a name for the instance file, select **Automatically generated**.
To choose a name, select **Specific name** and enter the name in the text box. To include variables, select them from the list beside the box.
 - c. To send a shortcut to the instance, select **Shortcut**. If you would like to send a copy of the instance, select **Copy**.
7. Set your other scheduling options and click **Schedule**.

Choosing a format

You can select the format that the document or report instance will be saved in when it is generated. This format will be saved to the destination you have selected. You can select from the formats summarized in the following table.

Table 23-6: Instance formats

Product	Format	Notes
Web Intelligence	<ul style="list-style-type: none"> • Web Intelligence • Microsoft Excel • Adobe Acrobat • Plain text • Rich text 	
Desktop Intelligence	<ul style="list-style-type: none"> • Desktop Intelligence • Microsoft Excel • Adobe Acrobat • Plain text • Rich text 	

Product	Format	Notes
Crystal Reports	<ul style="list-style-type: none"> • Crystal Reports • Microsoft Excel • Microsoft Excel (Data Only) • Microsoft Word (RTF) • PDF • Rich Text • Microsoft Word - Editable (RTF) • Plain Text • Paginated Text • Tab-separated Text • Separated Values • XML 	

Product	Format	Notes
		<ul style="list-style-type: none">• The difference between Excel and Excel (Data only) is that Excel attempts to preserve the look and feel of your original report, while Excel (Data only) saves only the data, with each cell representing a field.• The Tab-separated Values format places a tab character between values; the Separated Values format places a specified character between values.• If you choose to print the report when it is scheduled (by checking the Print in Crystal Reports format using the selected printer when scheduling check box on the Print Setup page), the report instance is automatically sent to the printer in Crystal Reports format. This does not conflict with the format you select when scheduling the report.• For Excel, Paginated Text, Tab-separated Values, and Character-separated Values, you specify certain formatting properties for the report. For example, if you select Character-separated Values, you can enter characters for the separator and

Product	Format	Notes
		delimiter; you can also select the two check boxes: Same number formats as in report and Same date formats as in report .

Related Topics

- [Selecting a destination](#)

To select a format for the report

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Actions** > **Schedule** and access the "Format" page.
 - If you are scheduling a Crystal report, click **Format**.
 - If you are scheduling a Desktop Intelligence document, click **DestinationFormat**.
 - If you are scheduling a Web Intelligence document, click **Formats and Destinations**.
3. Select the appropriate format.
 - If you are scheduling a Crystal report, choose the format from the list and click **Switch**. Some Crystal reports formats have other parameters that you can set when you schedule them.
 - If you are scheduling a Desktop Intelligence or Web Intelligence document, select your preferred format under "Output Format".
4. Set the rest of your scheduling options and click **Schedule**.

Related Topics

- [Additional formatting options for Crystal reports](#)

Additional formatting options for Crystal reports

When you schedule a Crystal report to some formats, you may be required to set additional options. This topic details the additional options for each format to which they apply:

- "Microsoft Excel (97-2003)"
- "Microsoft Excel (97-2003) (Data Only)"
- "Microsoft Word (97-2003)"
- "PDF"
- "Rich Text Format (RTF)"
- "Microsoft Word - Editable (RTF)"
- "Plain Text"
- "Paginated Text"
- "Separated Values (CSV)"
- "XML"

Table 23-7: Microsoft Excel (97-2003)

Option	Description
Use the export options defined in the report	To use the export options already defined in the report, select this option. You will not be able to set any of the other additional formatting options.
Set Column Width	<ul style="list-style-type: none">• To set the widths of Excel columns based on objects in the report, select Column with based on objects in the report and choose a report area from which to take the column widths.• To set a constant column width, select Constant column width (in points) and type the width.

Option	Description
Export page header and page footer	<ul style="list-style-type: none"> To include the page headers and footers in your instance, choose whether you would like to export them Once Per Report, or On Each Page. To exclude the page headers and footers from your instance, choose None.
Create page breaks for each page	Select this option to create page breaks.
Convert date values to strings	Select this option to export date values as text strings.
Show gridlines	Select this option to see gridlines in your exported document.
Page range	<ul style="list-style-type: none"> To include all pages of the report, select All. To include a page range, select from: and type the first page you want to include, and type the last page you want to include in the to: field.

Table 23-8: Microsoft Excel (97-2003) (Data Only)

Option	Description
Use the export options defined in the report	To use the export options already defined in the report, select this option. You will not be able to set any of the other additional formatting options.

Option	Description
Set Column Width	<ul style="list-style-type: none"> To set the widths of Excel columns based on objects in the report, select Column with based on objects in the: and choose a report area from which to take the column widths. To set a constant column width, select Constant column width (in points) and type the width.
Export object formatting	Select this option if you wish to preserve the object formatting.
Export images	Select this option to export the images in your report.
Use worksheet functions for summaries	Select this option to use summaries in the report to create worksheet functions in Excel.
Maintain relative object position	Select this option to maintain the positioning of objects relative to one another.
Maintain column alignment	Select this option to preserve the alignment of text within columns of your report.
Export page header and page footer	Select this option to include the header and footer in your instance.
Simplify page headers	Select this option to simplify page headers.

Option	Description
Show group outlines	Select this option to show group outlines.

Table 23-9: Microsoft Word (97-2003)

Option	Description
Page Range	<ul style="list-style-type: none"> To include all pages of the report, select All. To include a page range, select from: and type the first page you want to include, and type the last page you want to include in the to: field.

Table 23-10: PDF

Option	Description
Use the export options defined in the report	To use the export options already defined in the report, select this option. You will not be able to set any of the other additional formatting options.
Page Range	<ul style="list-style-type: none"> To include all pages of the report, select All. To include a page range, select from: and type the first page you want to include, and type the last page you want to include in the to: field.
Create bookmarks from group tree	Select this option to create bookmarks in your PDF file based on the tree structure of the report. This will make the report easier to navigate.

Table 23-11: Rich Text Format (RTF)

Option	Description
Page Range	<ul style="list-style-type: none">To include all pages of the report, select All.To include a page range, select from: and type the first page you want to include, and type the last page you want to include in the to: field.

Table 23-12: Microsoft Word - Editable (RTF)

Option	Description
Use the export options defined in the report	To use the export options already defined in the report, select this option. You will not be able to set any of the other additional formatting options.
Page Range	<ul style="list-style-type: none">To include all pages of the report, select All.To include a page range, select from: and type the first page you want to include, and type the last page you want to include in the to: field.
Insert page break after each report page	Select this option to insert page breaks in your RTF file after each page of the report.

Table 23-13: Plain Text

Option	Description
Number of characters per inch	Type a value between 8 and 16 for the number of characters to include per inch. This setting controls how the text file is displayed and formatted.

Table 23-14: Paginated Text

Option	Description
Use the export options defined in the report	To use the export options already defined in the report, select this option. You will not be able to set any of the other additional formatting options.
Number of lines per page	Type the number of lines of text to include between page breaks.
Number of characters per inch	Type a value between 8 and 16 for the number of characters to include per inch. This setting controls how the text file is displayed and formatted.

Table 23-15: Separated Values (CSV)

Option	Description
Use the export options defined in the report	To use the export options already defined in the report, select this option. You will not be able to set any of the other additional formatting options.

Option	Description
Delimiter	Type the character you want to use as the delimiter.
Separator	Type a character to use to separate values, or select Tab .
Mode	Select either standard or legacy mode. In standard mode, you can choose report, page, and group sections to include in your instance. In legacy mode, you cannot set those options.
Report and page sections	If you selected standard mode, indicate whether you want to export report and page sections, and if so, whether or not you want to isolate them.
Group sections	If you selected standard mode, indicate whether you want to export group sections, and if so, whether or not you want to isolate them.

Table 23-16: XML

Option	Description
XML Exporting formats	Select the XML exporting format you wish to use.

Selecting cache options for Web Intelligence or Desktop Intelligence documents

When the system runs a scheduled Web Intelligence or Desktop Intelligence document it stores the instance it generates on the Output File Repository

Server. In addition, you can choose to have the system cache the report on the appropriate Report Server by selecting a cache format for the document. If you don't select a cache format, then the system won't cache the document when it runs the document.

Note:

To select a cache option, the output format you specified for the object must be Web Intelligence or Desktop Intelligence. If you select a different format, the cache options you specify will have no affect.

To select a cache format for Web Intelligence or Desktop Intelligence documents

1. In the "Folders" management area of the CMC, select a Web Intelligence or Desktop Intelligence object.
2. Click **Actions** > **Schedule** and click **Caching**.
3. Select the format you want to pre-load the cache with.
4. Select the locale(s) with which to pre-load the cache if you are scheduling a Web Intelligence document.

When you schedule the Web Intelligence document, BusinessObjects Enterprise generates cached versions of the document in the locale(s) that you specify.

5. Set the rest of your scheduling options and click **Schedule**.

Scheduling an object for a user or group

The Schedule For feature allows you to generate reports that contain data for specific users only. It is intended to be used for either of the following types of objects:

- Crystal reports that are based on Business Views.
- Web Intelligence documents that use Universes.

Using the Schedule For feature you can schedule an object and specify for which users you want the system to run the object. The system will run the object and generate multiple instances of the report or document. Each instance will contain data that is relevant to the individual user only.

For example, you can schedule a sales report and on the Schedule For page you can specify the user names of all of your sales representatives. At the specified time, the system runs the report object and generates the individual report instances. Each instance would contain sales information for the individual sales representative only.

To change the Schedule For settings for an object

1. In the "Folders" management area of the CMC, select a report object.
2. Click **Actions > Schedule**.
3. On the navigation list, click **Schedule For**.
4. Select who you want to schedule the object for.
 - **Schedule only for myself**
 - **Schedule for specified users and user groups**
5. If you selected **Schedule for specified users and user groups**, navigate to and select the users and groups you would like to schedule for and click > to add them to the **Selected** list.

Tip:

If you need to remove users or groups from **Selected** list, select them and click <.

6. Set the rest of your scheduling options and click **Schedule**.

Selecting server group settings

You can indicate a specific server on which a scheduling will run. This gives you more control over load balancing; for instance, you may wish to run program jobs on a specific server group so that they do not monopolize system resources.

You can also choose a server group for BusinessObjects Enterprise to use when a user refreshes a Crystal report, Web Intelligence, or Desktop Intelligence instance while viewing it. These settings are accessed from the "Schedule" or "Default Settings" dialog boxes. For Crystal reports, click **Viewing Server Group**. For Web Intelligence documents, click **Webi Process Settings**. For Desktop Intelligence documents, click **Deski Process Settings**.

To select a server for your scheduling job

1. In the "Folders" management area of the CMC, select the object you wish to schedule.
2. Click **Actions > Schedule**.
3. On the navigation list, click **Scheduling Server Group**.
4. Select the appropriate option:
 - Choose **Use the first available server** to run the object as quickly as possible, regardless of server groups.
 - Choose **Give preference to servers belonging to selected group** if you would like to use a specific server group over another in the event that both are available.
 - Choose **Only use servers belonging to the selected group** to ensure that the job runs on the specified server group.

Note:

If you are scheduling a program object that requires access to files stored locally on a Program Job Server, but you have multiple Program Job Servers, you must specify which server to use to run the program.

5. Select or deselect **Run at origin site** to run the object where it is located.
6. Set the rest of your scheduling options and click **Schedule**.

Managing instances

To view or manage instances for a specific object, go to the "History" dialog box for the object. That page lists the scheduled instances and the output instances for an object:

- Scheduled instances will have a status of Recurring or Pending. The system has not yet run these instances, and the instances do not contain any data yet.
- Output instances, that is, actual report or program instances, will have a status of Success or Failed, which indicate whether they were run successfully:
 - A report instance contains actual report data.
 - A program instance stores the program's standard out and standard error in a text output file.

From the "History" dialog box, you can also choose to delete, run, pause, and refresh instances.

To manage storage space, it is good practice to limit the number of possible instances for an object, or to provide a time limit for the instances.

You can also manage instances for your entire BusinessObjects Enterprise deployment in one location called the "Instance Manager". This makes it much easier to, for example, see all failed instances and reschedule them.

Related Topics

- [Managing and viewing the history of instances](#)
- [Setting instance limits for an object](#)
- [Instance Manager](#)

Managing and viewing the history of instances

There are two ways to manage instances in BusinessObjects Enterprise. The "Instance Manager" lets you manage all of the instances on the system from one location.

The "History" dialog box displays all of the instances for a selected object. You can pause, resume, reschedule, **Run Now**, refresh, and delete instances from both locations. Rescheduling an instance preserves all the scheduling options for the initial scheduling job, and sets job to run immediately by default, but allows you to edit the scheduling options and run time. **Run Now** preserves all of the original scheduling options and sets the job to run immediately, but does not allow you to edit any scheduling options.

When you reschedule completed instances, a new scheduling job is created. However, if you reschedule a pending instance, you can indicate whether you want to initiate a new scheduling job or update the pending job. When you use **Run Now**, a new scheduling job is created regardless of the status of the instance.

The "History" dialog box and "Instance Manager" display slightly different information about each object. On the "History" dialog box, the Instance Time column displays the time and the date of the last update for each instance and the Title column displays the title of the instances. The Status column displays the status of each instance. The Run By column indicates which user scheduled the instance.

For report objects, the Format column displays which format the report is, or will be stored in and the Parameters column indicates what parameters were or will be used for each instance. For program objects, the Arguments column lists the command-line options that were or will be passed to the command line interface for each instance.

In the "Instance Manager", the Title column displays the title of the instance. The Status column displays whether or not the instance is pending, successful, or failed. The folder path displays to location of the instance. The Owner column displays the name of the user who scheduled the object. The Completion Time column displays the date and time when the instance completed its run, and the Next Run Time column displays the next time the object will be run, if it is on a recurring schedule and has a status of pending. The Server column displays the server on which the instance was run. The Error column displays any errors that occurred during the run that caused the object to fail.

BusinessObjects Enterprise creates instances from objects. That is, a report instance is created when a report object is scheduled and run by the Job Server. Essentially, a report instance is a report object that contains report data that is retrieved from one or more databases. Each instance contains data that is current at the time the report is processed. You can view specific report instances on the "History" dialog box of the report object.

BusinessObjects Enterprise creates a program instance each time that a program object is scheduled and run by the Program Job Server. Unlike report instances, which can be viewed in their completed format, program instances exist as records in the object history. BusinessObjects Enterprise stores the program's standard output and standard error in a text output file. This file appears when you click a program instance in the object "History".

Related Topics

- [To view an instance](#)
- [Pausing or resuming an instance](#)
- [To delete an instance](#)

To manage instances

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions > History**.
3. Select an instance or instances.

Note:

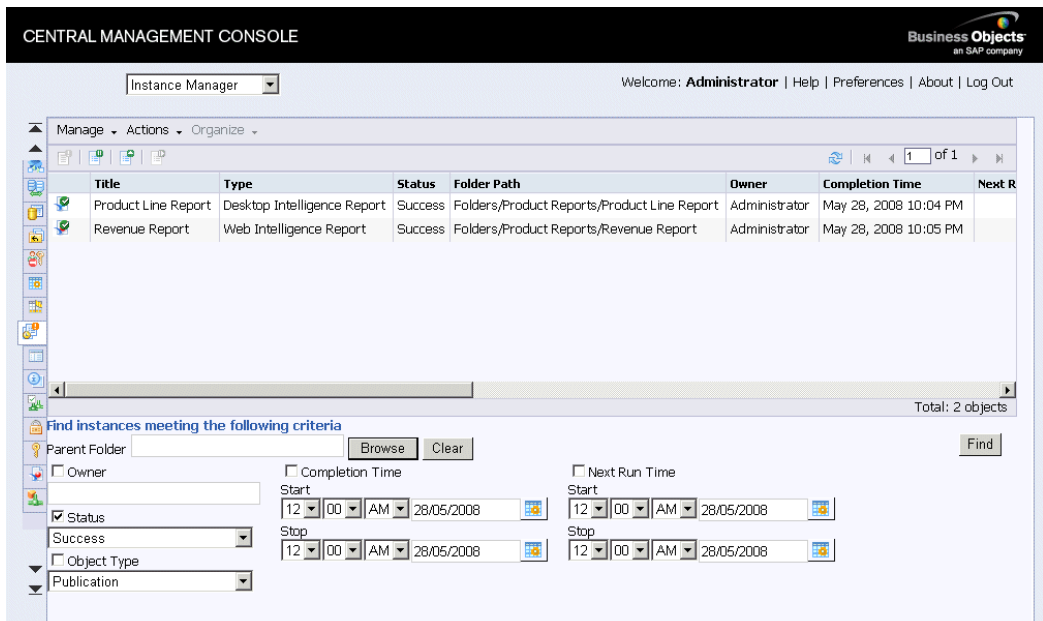
To refresh the list, click **Refresh**. In this case you don't need to select an instance first.

4. Click either **Run Now**, **Pause**, **Resume**, **Send to, Reschedule**, or **Delete**.

If you click **Run Now**, the system schedules the object to be run immediately. The scheduled job will have a status of Pending.

Instance Manager

The "Instance Manager" lets you view and manage all of the instances in your BusinessObjects Enterprise deployment from one location.



The default view of the "Instance Manager" shows all pending instances, sorted by title. You can filter your view to see only relevant instances. You can filter by:

- Parent folder
- Owner

- Status
- Object type
- Completion time
- Next run time

You can multi-select instances to perform batch operations on them, such as pause, resume, or delete. You can also use the Instance Manager to request detailed information for a single instance, which can be helpful when you use the "Instance Manager" to diagnose and resolve system problems that cause instances to fail.

For example, 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 of the 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 re-run all of the failed jobs.

Note:

To view detailed information about an instance, select the instance and click the **Instance details** icon in the toolbar.

Finding instances in the Instance Manager

You can enter filters to find specific instances in the "Find instances meeting the following criteria" section of the "Instance Manager". You can base filters on the following criteria:

Criteria	Description
Parent Folder	Enable this criterion and browse for a BusinessObjects Enterprise folder to list all instances that are children of the folder.
Owner	Enable this criterion and type a BusinessObjects Enterprise user name to list instances scheduled by that user.
Status	Enable this criterion to list instances of the status you choose from the drop-down list; you can choose to list either successful, failed, running, paused or pending instances.
Object type	Enable this criterion to list instances of the object type you choose from the drop-down list.
Completion time	Enable this criterion to list instances that were completed between the “start” and “stop” date and times that you enter. Note: For completed publication instances, it is recommended that you enable Object Type and set it to Publication as well as setting the completion time.
Next run time	Enable this criterion to list instances that have their next run between the “start” and “stop” date and times that you enter.

To enable a criterion, you must ensure that the checkbox beside it is selected. When you have entered all of the criteria, click **Find**. Only instances that meet all the criteria you have enabled will be displayed.

Note:

When you schedule an object to Business Objects inboxes, the documents that users receive in their inboxes are not considered instances. Therefore, these inbox documents do not appear in the Instance Manager.

Viewing instances

The Instance Manager displays the following information about instances: **Title**, **Object Type**, **Status**, **Folder Path**, **Owner** (the user who scheduled the job), **Completion time**, **Next run time**, **Submission time**, **Start time**, **Duration**, **Recurrence** (how often a new instance is created), **Expiry** (when the job is no longer valid), **Server**, and **Error** (displays an error message if the instance fails).

To view an instance

1. Select an object in the "Folders" management area of the CMC.
2. Click **Actions > History**.
3. In the **Instance Time** column, click the instance you want to view.

You can also use the "Instance Manager" to view a list of instances by status or by user.

You will need to scroll to the right in order to view all the columns with default width.

Note:

You cannot sort instances using the Submission time, Start time, Duration, Recurrence, or Expiry columns.

Related Topics

- [Instance Manager](#)

Pausing or resuming an instance

You can pause and then resume an instance as needed. Pause and resume can be applied to scheduled instances only (that is, instances that have a status of Recurring or Pending).

For example, if a job server is down for maintenance reasons, you may want to pause a scheduled instance. This prevents the system from running the object, and the object from failing because the job server is not running. When the job server is running again, you can resume the scheduled object.

To pause an instance

1. Go to the "History" dialog box for an object.
2. Select the scheduled instance you want to pause.
3. Click **Pause**.

To resume a paused instance

1. Go to the "History" dialog box for an object.
2. Select the scheduled instance you want to resume.
3. Click **Resume**.

To delete 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 or failed.

1. Go to the "History" dialog box for an object.
2. Select the instance or instances you want to delete.
3. Click **Delete**.

Setting instance limits for an object

In the "Limits" page, you can set the limits for the selected object and its instances. You set limits to automate regular clean-ups of old BusinessObjects Enterprise content. At the object level, you can limit the number of instances that remain on the system for the object or for each user or group; you can also limit the number of days that an instance remains on the system for a user or group.

In addition to setting the limits for the objects from the "Folders" management area, you can also set limits at the folder level. When you set limits at the folder level, these limits will be in effect for all objects that reside within the folder (including any objects found within the subfolders).

Note:

When you set the limits at the object level, the object limits will override the limits set for the folder; that is, the object will not inherit the limits of the folder.

Related Topics

- [Setting limits for folders, users, and groups](#)

To set limits for instances

1. In the "Folders" management area of the CMC, select an object.
2. Click **Actions > Limits**.

The "Limits" dialog box appears.

3. Make your settings according to the types of limits you want to set for your instances. The options are as follows:

- **Delete excess instances when there are more than N instances of an object**

To limit the number of instances per object, select this check box. Then, type the maximum number of instances that you want to remain on the system. (The default value is 100.)

- **Delete excess instances for the following users/groups**

To limit the number of instances for users or groups, click **Add** in this area. Select from the available users and groups and press > to add them to your list. Then click **OK**. Type the maximum number of instances in the **Instance Limit** column. (The default value is 100.)

- **Delete instances after N days for the following users/groups**

To limit the number of days that instances are saved for users or groups, click **Add** in this area. Select from the available users and groups and press > to add them to your list. Then click **OK**. Type the maximum age of instances in the **Maximum Days** column. (The default value is 100.)

4. Click **Update**.

Using calendars

Calendars overview

Calendars make it easy for you to schedule complex recurring jobs efficiently. A calendar is a customized list of run dates for scheduled jobs. When users schedule objects, they can use a calendar to run the job on a predefined set of dates. By providing calendars for your users, you can create more complex processing schedules than you can with the standard scheduling options.

Calendars are particularly useful when you want to run a recurring job on an irregular schedule, or if you want to provide users with sets of regular scheduling dates to choose from. Calendars also allow you to create more complex processing schedules, combining unique scheduling dates with recurring ones.

For example, if you want a report object to run every business day except for your country's statutory holidays, you can create a calendar with the holidays marked as "non-run" days, on which the report object cannot be run. BusinessObjects Enterprise will run the job every day you have specified as a "run" day in your calendar.

You can set up as many calendars as you want in BusinessObjects Enterprise. Calendars you create appear in the Calendar selection list available when you choose to schedule an object using a calendar. When you apply the calendar to a job, BusinessObjects Enterprise runs the job on the run dates as scheduled.

You can apply calendars to any object that can be scheduled, including report objects, program objects, and object packages.

Creating calendars

In the CMC, go to the "Calendars" management area to create new calendars and to modify existing calendars. To create a calendar, you need to provide a name and description. When the calendar is created, you can add run dates to it using the Dates tab.

Tip:

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.

To create a calendar

1. Go to the "Calendars" management area of the CMC.
2. Click **Manage > New > New Calendar**.
3. Type a name and description for the new calendar.
4. Click **OK**.

The new calendar is added to the system. You can now add run dates to this calendar.

Related Topics

- [Adding dates to a calendar](#)

Adding dates to a calendar

You can add dates to a calendar using a number of different formats. You can choose specific dates using a yearly, quarterly, or monthly view of the calendar, or you can choose recurring dates using general formats based on the day of the month or week.

To add dates to a calendar

1. Go to the "Calendars" management area of the CMC.
2. Select the calendar you want to change.
3. Click **Actions > Select Dates**.
4. Click the days of the month that you want to include as run days for the calendar.

To remove a run day, click the day again.

Tip:

To select a week, or all of the particular weekdays in a month, you can click the row or column header.

5. To add the new dates to the calendar, click **Save**.

Note:

When you change an existing calendar, BusinessObjects Enterprise checks all currently scheduled instances in your system. Objects that use the edited calendar are automatically updated to run on the revised date schedule.

Calendar format options

Calendar format option	Description
Yearly	Yearly displays the calendar's run dates for the year. To change the year displayed, you can click the Previous year and Next year buttons. To add a date from the Yearly format, click the day, weekday header, or week row header that you want to add.
Quarterly	Quarterly displays the calendar's run dates for the current calendar quarter. You can change the displayed quarter using the Previous quarter and Next quarter buttons. To add a date from the Quarterly format, click the day, weekday header, or week row header that you want to add.

Calendar format option	Description
Monthly	Monthly displays the calendar's run dates for the current month. You can change the displayed month using the Previous month and Next month buttons. To add a date from the Monthly format, click the day, weekday header, or week row header that you want to add.

Specific dates

To add a specific date to a calendar, use the **Yearly**, **Quarterly**, and **Monthly** formats to add dates to the calendars.

The **Yearly** format displays the run schedule for the entire year. The **Quarterly** format displays the run dates for the current quarter. You can also view the **Monthly** format for the calendar, which displays the run dates for the current month. In all three formats, you can change the displayed time range by clicking the previous and next buttons.

You can add specific dates in any calendar format by clicking on the day you wish to add. If you wish to add an entire week, click > in the row header for that week. To add run days on all of a given day of the week in a month, click the name day of the week.

2008 - 2009 Previous year Next year

Add recurring days: By day of month By day of week View: **Yearly** Quarterly Monthly

Add or remove run days by clicking on the dates below.

Click on the header to toggle a specific day of the week, or click on the row header on the left to toggle a whole week.

May 2008							June 2008							July 2008							
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
>				1	2	3	>	1	2	3	4	5	6	7	>		1	2	3	4	5
>	4	5	6	7	8	9	>	8	9	10	11	12	13	>	6	7	8	9	10	11	
>	11	12	13	14	15	16	>	15	16	17	18	19	20	>	13	14	15	16	17	18	
>	18	19	20	21	22	23	>	22	23	24	25	26	27	>	20	21	22	23	24	25	
>	25	26	27	28	29	30	>	29	30					>	27	28	29	30	31		

August 2008							September 2008							October 2008						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
>					1	2	>	1	2	3	4	5	6	>			1	2	3	4
>	3	4	5	6	7	8	>	7	8	9	10	11	12	>	5	6	7	8	9	10
>	10	11	12	13	14	15	>	14	15	16	17	18	19	>	12	13	14	15	16	17
>	17	18	19	20	21	22	>	21	22	23	24	25	26	>	19	20	21	22	23	24
>	24	25	26	27	28	29	>	28	29	30				>	26	27	28	29	30	31

> 31 Save Save & Close Reset Cancel

Legend

- 8 Non-run day
- 8 Original run day
- 8 New run day
- 8 Removed run day

For example, if your company ships products according to an irregular schedule that cannot be defined using the daily or weekly settings, you can create a list of these dates in a "Shipping dates" calendar. The Shipping department can now check the inventory after each shipment by scheduling a report that uses the calendar to run at the end of each shipping day.

Related Topics

- [Recurring dates](#)

Recurring dates

You can add recurring days based on the day of the week or the day of the month. To view existing run dates, you must use the **Yearly**, **Quarterly**, or **Monthly** format; the generic formats must be used to add recurring dates to the calendar. To add the recurring days, click **By day of month** or **By day of week** and select the days you wish to add.

Although you can set a recurring schedule using the standard scheduling options, calendars allow you to specify several different recurring run patterns

at once. You can also run instances on dates that do not follow the pattern by adding individual days to a calendar.

For example, to schedule a report object to run on the first four days of every month, and on the second and fourth Friday of every month, first create a new calendar object and name it. Then, choose to add recurring days by day of month to add the first four days of the month to this calendar. When you update the calendar, the Yearly format appears with the new run dates.

Add recurring days by day of month

Add recurring days: **By day of month** By day of week

Add monthly recurring run days by clicking on the days of month below.

Start Date: ☒ 2008/05/26

End Date: ☐ 2009/05/26

Legend

Non-run day

New run day

Days of month

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

To add every second and fourth Friday to the calendar, choose to add recurring days by day of week and select the second and fourth Friday.

Add recurring days by day of week

Add recurring days:

Add monthly recurring run days by clicking on the days of week below.



Click on the header to toggle a specific day of the week, or click on the row header on the left to toggle a whole week.

Start Date: ☒ End Date: ☐ 

Days of week

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
> First	First	First	First	First	First	First	First
> Second	Second	Second	Second	Second	Second	Second	Second
> Third	Third	Third	Third	Third	Third	Third	Third
> Fourth	Fourth	Fourth	Fourth	Fourth	Fourth	Fourth	Fourth
> Last	Last	Last	Last	Last	Last	Last	Last

Legend

 8 Non-run day 8 New run day

Deleting calendars

When you delete a calendar, any objects that are scheduled according to the deleted calendar will be run one more time by the system. After that, the system won't be able to schedule the objects again, because the calendar no longer exists. To ensure the objects continue to be run, change the scheduling information for the objects either by selecting a different calendar or a different recurrence pattern.

Related Topics

- [To schedule an object](#)

To delete a calendar

1. Go to the "Calendars" management area of the CMC.

2. Select the calendar you want to delete.

Tip:

Select multiple calendars by holding down the **CTRL** or **SHIFT** key and clicking on them to delete them simultaneously.

3. Click **Manage > Delete**.
4. Click **OK** to confirm.

Specifying calendar rights

You can grant or deny users and groups access to calendars. Depending how you organize your calendars, you may have specific sets of dates that you want to be available only for certain employees or departments. For example, your finance team may use a series of financial tracking dates that aren't useful for other departments. Users will be able to see only the calendars they have the rights to see, so you can use rights to hide calendars that aren't applicable to a particular group.

By default, calendars are based on current security settings, inheriting rights from the users' parent folders.

Related Topics

- [To assign principals to an access control list for an object](#)

Managing events

Managing events overview

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. This section shows how to create events in the "Events" management area of the CMC.

You can create three kinds of events:

- **File events**

When you define a file-based event, you specify a filename that the Event Server should monitor 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.

- **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.

- **Custom events**

When you create a custom event, you create a shortcut for triggering an event manually.

When working with events, keep in mind that an object's recurrence schedule still determines how frequently the object runs. For instance, a daily report that is dependent upon a file-based event will run, at most, once a day (so 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.

Related Topics

- [File-based events](#)
- [Schedule-based events](#)
- [Custom events](#)
- [Scheduling an object with events](#)

File-based events

File-based events wait for a particular file (the trigger) to appear before the event occurs. Before scheduling an object that waits for a file-based event to occur, you must first create the file-based event in the "Events"

management area of the CMC. Then, you can schedule the object and select this event.

File-based events are monitored by the Event Server. When the file that you specify appears, the Event Server triggers the event. The Central Management Server then releases any schedule requests that are dependent on the event.

For instance, suppose that you want your daily reports to run after your database analysis program has finished and written its automatic log file. To do this, you specify the log file in your file-based event, and then schedule your daily reports with this event as a dependency. When the log file appears, the event is triggered and the reports are processed.

Note:

If the file already exists prior to the creation of the event, the event is not triggered. In this case, the event is triggered only when the file is removed and then recreated. If you want an event to be triggered multiple times, you must remove and recreate the file each time.

Related Topics

- [Scheduling an object with events](#)

To create a file-based event

1. Go to the "Events" management area of the CMC.
2. Click **Manage > New > New Event**.
3. In the **Type** list, select **File**.
4. Type a name for the event in the **Event Name** field.
5. Complete the **Description** field.
6. In the **Server** list, select the Event Server that will monitor the specified file.
7. Type a file name in the **Filename** field.

Note:

Type 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.

8. Click **Create**.

Schedule-based events

Schedule-based events are dependent upon scheduled objects. That is, a schedule-based event is triggered when a particular object has been processed. When you create this type of event, it can be based on the success or failure of a scheduled object, or it can be based simply on the completion of the job.

Most importantly, you must associate your schedule-based event with at least two scheduled objects. The first object serves as the trigger for the event: when the object is processed, the event occurs. The second object is dependent upon the event: when the event occurs, this second object runs.

For instance, suppose that you want report objects R1 and R2 to run after program object P1 runs. To do this, you create a schedule-based event in the Events management area. You specify the **Success** option for the event, which means that the event is triggered only when program P1 runs successfully. Then, you schedule reports R1 and R2 with events, and select your new schedule-based event as the dependency. Schedule program P1 with events, and set program P1 to trigger the schedule-based event upon successful completion. Now, when program P1 runs successfully, the schedule-based event is triggered, and reports R1 and R2 are subsequently processed.

Related Topics

- [Scheduling an object with events](#)

To create a schedule-based event

1. Go to the "Events" management area of the CMC.
2. Click **Manage > New > New Event**.
The "New Event" dialog box appears.
3. In the **Type** list, select **Schedule**.
4. Type a name for the event in the **Event Name** field.
5. Complete the **Description** field.
6. Select an event status option.

Event status	Description
Success	The event is triggered only upon successful completion of a specified object.
Failure	The event is triggered only upon non-successful completion of a specified object.
Success or Failure	The event is triggered upon completion of a specified object.

7. Click **Create**.

Custom events

A custom event occurs only when you explicitly trigger it. As with all other events, an object based on a custom event runs only when the event is triggered within the time frame established by the object's schedule parameters. Custom events are useful because they allow you to set up a shortcut that, when clicked, triggers any dependent schedule requests.

Tip:

When developing your own web applications, you can trigger Custom events from within your own code, as required. For more information, see the developer documentation available on your product CD.

For instance, you may have a scenario where you want to schedule a number of reports, but you want to run them after you have updated information in your database. To do this, create a new custom event, and schedule the reports with that event. When you update the data in the database and you need to run the reports, return to the event in the CMC and trigger it manually. BusinessObjects Enterprise then runs the reports.

Note:

You can trigger a custom event multiple times. For example, you might schedule two sets of event-based program objects to run daily—one set runs in the morning, and one set runs in the afternoon. When you first trigger the related custom event in the morning, one set of programs is run; when you trigger the event again in the afternoon, the remaining set of programs is

run. If you neglect to trigger the event in the morning and trigger it only in the afternoon, both sets of programs run at that time.

Related Topics

- [Scheduling an object with events](#)

To create a custom event

1. Go to the "Events" management area of the CMC.
2. Click **Manage > New > New Event**.
3. In the **Type** list, select **Custom**.
4. Type a name for the event in the **Event Name** field.
5. Complete the **Description** field.
6. Click **OK**.

Note:

Before you trigger this custom event, schedule an object that is dependent upon this event.

To trigger a custom event

1. Go to the "Events" management area of the CMC.
2. In the **Event Name** column, select a custom event.
3. Click **Actions > Trigger Event**.

Specifying event rights

You can grant or deny users and groups access to events. Depending how you organize your events, you may have specific events that you want to be available only for certain employees or departments. For example, you may want certain events to be triggered only by management or IT.

Users will only be able to see events they have the rights to see, so you can use rights to hide events that aren't applicable to a particular group. For example, by granting only the ITAdmin group access to IT-related events, those events won't appear for a user from the HRAdmin group; this makes the event list easier for the HRAdmin group to navigate.

By default, events are based on current security settings, inheriting rights from the users' parent folders.

Related Topics

- [*To assign principals to an access control list for an object*](#)

To run objects now

You can run objects in bulk from the "Folders" management area of the CMC using **Run Now**. When you run objects now, they are automatically scheduled to run right away using their default scheduling settings.

1. Go to the "Folders" management area of the CMC.
2. Navigate to the object(s) that you want run and select them.
3. Click **Actions** and **Run Now**.



Organizing Objects

24

chapter



Overview

This section describes basic administration tasks for organizing your files. It shows how to add folders and categories, and how to change settings, such as object rights and limits for new folders and categories, and make some common changes to the system's default security settings.

Related Topics

- [Organizing objects overview](#)
- [Working with folders](#)
- [Working with categories](#)

Organizing objects overview

Creating an intuitive and logical organizational structure is the key to ensuring that your users can find the information they need quickly and easily. BusinessObjects Enterprise provides two methods for organizing content: folders and categories. By using folders and categories, and setting appropriate rights for them, you can organize data according to multiple criteria and improve both security and navigation.

About folders

Folders are objects used to organize documents. You can use folders to separate content into logical groups. Because you can set security at the folder level, you can use folders as a tool for controlling access to information.

It's good practice to set up folders that represent a structure that already exists in your organization, such as departments, regions, or even your database table structure. Then use categories to set up an alternate system of organization.

Each object in BusinessObjects Enterprise must reside in a folder. By default, new objects that you add to a folder inherit the object rights that are specified for the folder.

About categories

Categories provide an alternative way of organizing objects, and therefore an alternative way for users to navigate to them. For example, you could organize your content into departmental folders, and then use categories to create an alternate filing system that divides content according to different roles in your organization, such as managers or VPs. This organizational model allows you set security on groups of documents based on department or job role.

There are two types of categories: corporate and personal. Corporate categories are created and administrated by administrators with the appropriate rights, and are only visible to groups and users who have the rights to view them; personal categories are created by individual users, and are only visible to themselves.

While all objects must reside in folders, category assignment is optional; therefore, it is important to note that:

- While you can assign rights to a category as an object (that is, grant groups and users rights to it), the objects within the category cannot inherit rights set on the category itself.
- An object in a category retains its affiliation with the folder it resides in.
- An object can reside in multiple categories.

Working with folders

Folders are objects used to organize documents. You can use folders to separate content into logical groups. Because you can set security at the folder level, you can use folders as a tool for controlling access to information.

Creating and deleting folders

There are several ways to create new folders in BusinessObjects Enterprise. In the Central Management Console (CMC), go to the "Folders" management area to create new folders and to add subfolders to the existing hierarchy of folder objects.

Tip:

When you publish local directories and subdirectories of reports with the Publishing Wizard, you can duplicate your local directory structure on the BusinessObjects Enterprise system. This method provides you with an efficient way of creating multiple folders and subfolders at the same time.

Related Topics

- [Overview](#)
- [To create a new folder](#)
- [To delete folders](#)

To create a new folder

To create a top level folder, ensure that you are viewing **All Folders** when you create your new folder. To create a subfolder, navigate to the folder in which you would like to create the new folder and then create it.

This procedure shows how to create a new folder at any level of your folder hierarchy.

1. Go to the "Folders" management area of the CMC.
2. Navigate to the location in which you would like to create the folder.
3. Click **Manage > New > Folder**.
4. Type the name, description, and keywords of your new folder.

Tip:

To edit this information later, select the folder, click **Manage** and choose **Properties**.

5. Click **OK**.

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

To delete folders

When you delete a folder, all subfolders, reports, and other objects contained within it are removed entirely from the system.

1. Go to the "Folders" management area of the CMC.
2. Select the folder that you want to delete in the Details panel.

Tip:

To select multiple folders, hold down the **CTRL** or **SHIFT** key and click each folder, so that you can delete several folders simultaneously.

3. Click **Manage > Delete**.
4. Click **OK** to confirm that you wish to delete the folder.

Copying and moving folders

When you copy or move a folder, the objects contained within it are also copied or moved. BusinessObjects Enterprise treats the folder's object rights differently, depending upon whether you copy or move the folder:

- When you copy a folder, the newly created folder does not retain the object rights of the original. Instead, the copy inherits the object rights that are set on its new parent folder. For instance, if you copy a private Sales folder into a Public folder, the contents of the new Sales folder will be accessible to all users who have rights to the Public folder.
- When you move a folder, all of the folder's object rights are retained. For instance, if you move a private Sales folder into a publicly accessible folder, the Sales folder will remain inaccessible to most users.

To copy or move a folder

1. Go to the "Folders" management area of the CMC.
2. Select the folder that you want to copy or move.

If the folder you want to copy or move is not at the top level, locate its parent folder. Then make your selection on the parent folder contents.

Tip:

To select multiple folders, hold down the **CTRL** or **SHIFT** key and click each folder, so that you can move several folders simultaneously.

3. Click **Organize > Copy To** or **Organize > Move To**.
4. Select the destination folder from the list and click **>** to add it to the **Destinations** list.
5. Click **OK**.

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

Adding new objects to a folder

To add a Crystal report to a folder

1. Navigate to the folder and click **Manage > Add > Crystal Reports**.

Note:

If you view a folder with subfolders and add a report while you have a subfolder selected, the report will be added to the selected subfolder; not to the folder you are currently viewing.

2. Type a title and description for the report, or choose to use the description saved in the report.
3. Enter keywords for the report.
Keywords are used when searching for objects.
4. Click **Browse** and choose the report from your computer.
5. Indicate whether or not you would like to keep any saved data in the report.
6. Navigate to the categories you would like the report to belong to and select them.
7. Click **OK**.

To add a program object to a folder

1. Choose **Manage > Add > Program File**.
2. Click **Browse** and choose the program file from your computer.
3. Indicate the type of program you are adding (**Executable**, **Java**, or **Script**).
4. Click **OK**.

To add an object from your computer to a folder

1. Navigate to the folder and click **Manage > Add > Local Document**.

Note:

If you view a folder with subfolders and add an object while you have a subfolder selected, the object will be added to the selected subfolder; not to the folder you are currently viewing.

2. Click **Browse** and choose the object from your computer.
3. Choose the correct file type from the list.
If the file type you are adding does not appear in the list, choose **Other** and enter the MIME type of the file in the **MIME** field.
4. Click **General Properties** to rename the file, enter a description, or enter keywords.
5. When you are finished, click **OK**.

Specifying folder rights

You can change the object rights for a new folder that you have just created. By default, new objects that you add to a folder inherit the object rights that are specified for the folder.

Related Topics

- [To assign principals to an access control list for an object](#)
- [How rights work in BusinessObjects Enterprise](#)

Setting limits for folders, users, and groups

Limits allow you to delete report instances on a regular basis. You set limits to automate regular clean-ups of old BusinessObjects Enterprise content. Limits that you set on a folder affect all objects that are contained within the folder. At the folder level, you can limit the number of instances that remain on the system for each object or for each user or group; you can also limit the number of days that an instance remains on the system for a user or group.

Related Topics

- [Setting instance limits for an object](#)

To limit instances at the folder level

1. Select a folder and click **Actions > Limits**.
2. Modify the available settings according to the types of instance limits that you want to implement, and click **Update** after each change.

The available settings are:

- **Delete excess instances when there are more than N instances of an object**

- a. To limit the number of instances per object, select **Delete excess instances when there are more than N instances of an object**.
- b. Type the maximum number of instances that you want to remain on the system.

Note:

The default value is 100.

- **Delete excess instances for the following users/groups**

- a. To limit the number of instances per user or group, click **Add** in this area.
- b. Select from the available users and groups, click **>** to add the users or groups to the **Selected users/groups** list.
- c. Click **OK**.
- d. Type the maximum number of instances that you want to remain on the system.

Note:

The default value is 100.

- **Delete instances after N days for the following users/groups**

- a. To limit the age of instances per user or group, click **Add** in this area.
- b. Select from the available users and groups, click **>** to add the users or groups to the list of **Selected users/groups**.
- c. Click **OK**.
- d. Type the maximum age of instances in the **Maximum Days** column.

Note:

The default value is 100.

Managing Personal Folders

BusinessObjects Enterprise creates a folder for each user on the system. These folders are organized within the CMC as Personal Folders. By default, there are Personal Folders for the Administrator and Guest accounts. When you log on to the CMC and view the list of Personal Folders, you will see only those folders to which you have View access (or greater).

Within InfoView, these folders are referred to as the Favorites folders.

To view the Personal Folders

- Go to the "Personal Folders" management area of the CMC.

A list of subfolders appears. Each subfolder corresponds to a user account on the system. Unless you have View access (or greater) to a subfolder, it will not appear in the list.

Working with categories

Categories provide an alternate way to organize objects. You can associate documents with multiple categories, and you can create subcategories within categories.

BusinessObjects Enterprise provides two types of categories:

- Corporate categories are created by the administrator, or other users who have been granted access to these categories. If you have the appropriate rights, you can create administrative categories.
- Personal categories can be created by each user to organize their own personal documents.

To create a new category

1. Go to the "Categories" management area of the CMC.
2. Click **Manage > New > Category**.
3. Type a name for your category.
4. Click **OK**.

The new category is added to the system.

You can now click **Manage > Categories** to change settings for this category.

To delete categories

When you delete a category, all subcategories within it are removed entirely from the system. Unlike folder deletion, the reports and other objects contained within the category are not deleted from the system.

1. Go to the "Categories" management area of the CMC.
2. Select the category that you want to delete.

If the category you want to delete is not at the top level, locate its parent category. Then make your selection.

Tip:

To select multiple categories, hold down the CTRL or SHIFT key and click each category, so that you can delete several categories simultaneously.

3. Click **Manage** and choose **Delete**.
4. Click **OK** to confirm that you wish to delete the category.

To move a category

When you move a category, any object assigned to the category maintains its association with it. All of the category's object rights are retained.

For example, you may have a South American Sales category that is accessible only by sales people in that region. You also have a World Sales category that contains worldwide sales reports needed by all sales people. For more intuitive organization, you want to move the region categories into the World Sales category. When you move the South American Sales category into the World Sales category, it retains its rights settings and associated objects, even though it has become a subcategory of the World Sales category.

1. Go to the "Categories" management area of the CMC.
2. Select the category that you want move.

If the category you want to move is not at the top level, locate its parent category. Then make your selection.

Tip:

To select multiple categories, hold down the **CTRL** or **SHIFT** key and click each category, so that you can move several categories simultaneously.

3. Click **Organize > Move To**.
4. Select the destination category and add it to the **Destinations** list by clicking **>**.

Tip:

If there are many categories on your system, use the "Search title" field to search, or click Previous, Next, and **+** to browse the category hierarchy.

5. Click **OK**.

The category you selected is moved to the new destination.

To add an object to a category

Follow this procedure to add an object to a category.


1. Go to the "Folders" management area of the CMC.
2. Navigate to the object you would like to add to a category and select it.
3. Click **Manage > Categories**.
4. Select the categories to which you want to add the object.
5. Click **Save & Close**.

Related Topics

- [Overview](#)

To remove or delete objects from a category

You can either remove or delete objects from a category. When you remove an object, you remove it from the category only. When you delete an object, you remove it from the category and also delete it from the system.

1. Go to the "Categories" or "Personal Categories" management area of the CMC.
2. Double-click the category from which you want to remove or delete an object.
3. Select the object or objects you want to remove or delete.
4. Remove the object from the category or delete the object.
 -  Click **Remove** to remove the object from the category only. In this case, the object continues to exist in the system.
 - Click **Organize** and **Delete** to remove the object from the category and at the same time delete it from the system.

Specifying category rights

Follow this procedure to change the object rights for a category. By default, new objects that you add to a category inherit the object rights that are specified for the category.

Related Topics

- [Managing security settings for objects in the CMC](#)

To view the Personal Categories

If you are granted the appropriate rights, you can view, edit, and delete users' personal categories.

1. Go to the "Personal Categories" management area of the CMC.
2. Click the user account whose personal categories you want to view.

A list of the user's personal categories appears.

Related Topics

- [Account management overview](#)



Adding Objects to the Repository

25

chapter



Overview

This section discusses the process of adding objects to the BusinessObjects Enterprise environment and making them available to authorized users. There are several types of objects that you can add to BusinessObjects Enterprise:

- reports (from Crystal Reports)
- documents (from Desktop Intelligence and Web Intelligence)
- visualizations (from Crystal Xcelsius)
- Flash objects
- programs
- Microsoft Excel/Word/PowerPoint files
- PDFs
- text files
- rich text format files

You can add objects to BusinessObjects Enterprise in three ways: with the Publishing Wizard, through the CMC, and by saving objects directly to the CMS.

Note:

You can also create and add new objects directly to BusinessObjects Enterprise from within InfoView.

Options for adding Crystal reports

During the adding process, you specify how often a Crystal report is run. You can choose to set a recurring schedule, or you can choose to let users set the schedule themselves. You can specify whether the data in the report is automatically refreshed according to a set schedule or if the data is refreshed only when users manually refresh the report.

Each option has several features:

- Specifying the data that users see.

This option is recommended for objects that are accessed by a large number of people and/or do not require separate database logon credentials. When you add an object, users can access the same instance

of the object and reduce the number of times that the system is prompted for information.

- Allowing users to update the data in the report.

This option is recommended for objects that require separate database logon credentials. It is also recommended when you add smaller objects that have frequent data changes and/or make use of parameters and record selection formulas. When you add an object, users are able to determine the frequency in which the object is updated. However, users who access the object at the same time increase the load on the system by increasing the number of times that it is prompted for information.

Note:

BusinessObjects Enterprise supports reports that are created in versions 6 through XI of Crystal Reports, and in Crystal Reports 2008. However, once a report is added to BusinessObjects Enterprise, it is saved, processed, and displayed in version 2008 format.

Publishing Wizard procedures

The Publishing Wizard is a locally installed, Windows application that is made up of a series of dialog boxes. When you use the wizard, only the dialog boxes that are applicable to the objects/folders that you are adding appear. For example, the settings for parameters and schedule format do not appear when you add Voyager workspaces.

Use the Publishing Wizard if you have access to the application and you want to add multiple objects or an entire directory of objects to BusinessObjects Enterprise. Once an object is added, it appears in the folder that you specified in InfoView (or your customized web desktop) and in the "Folders" management area of the CMC.

To log on to BusinessObjects Enterprise via the Publishing Wizard

Before you can add an object, you need to log on to BusinessObjects Enterprise via the Publishing Wizard.

1. On Windows, click **Start > Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Publishing Wizard**.

The "Welcome to the Publishing Wizard" dialog box appears.

2. If you want the Publishing Wizard dialog boxes to display in a different language, select the language on the **Language** list.

The languages available on the **Language** list vary depending on your installation configuration.

3. Click **Next**.

The "Please Log On" dialog box appears.

4. In the **System** field, type the name of the CMS that you want to add objects to.
5. In the **User Name** and **Password** fields, type your BusinessObjects Enterprise logon credentials.
6. From the **Authentication** list, select the appropriate authentication type.
7. Click **Next**.

The "Select Files" dialog box appears.

To choose objects to add to the CMS

The Publishing Wizard lets you add the following types of objects to the repository:

- reports (from Crystal Reports)
- visualizations (from Crystal Xcelsius)
- Flash objects
- programs
- Microsoft Excel/Word/PowerPoint files
- PDFs
- text files
- rich text format files

For Desktop Intelligence and Web Intelligence documents, you must save the documents directly to the repository from within the document designer.

1. In the "Select Files" dialog box, click **Add Files** or **Add Folder**.
2. Select the file/folder that you want to add.

Tip:

- Ensure that the appropriate file type is selected from the list; by default this value is set to **Report (*.rpt)**.
 - If you are adding a folder, you can also add its subfolders by selecting the **Include Subfolders** check box.
3. Repeat steps 1 and 2 for each of the files/folders that you want to add.
 4. Click **Next**.
 5. If the "Specify Object Type" dialog box appears, choose a file type for each unrecognized object, and then click **Next**.

The "Specify Location" dialog box appears.

Related Topics

- [Saving objects directly to the CMS](#)

To create or select a folder in the CMS

To add the selected objects, you must create or select a folder on the host CMS. Only the folders to which you have access appear in the "Specify Location" dialog box.

1. In the "Specify Location" dialog box, select the folder where you want to add the objects.

To create a new folder in the CMS, select a folder and then click New Folder.



To create a new object package in the CMS, select a folder, and then click New Object Package.



To delete a folder or an object package, select the object, and click Delete.



Note:

From the wizard, you can delete only new folders and object packages. New folders are green; existing folders are yellow.

2. Click **Next**.

The "Confirm Location" dialog box appears.

Related Topics

- [To duplicate the folder structure](#)
- [To move objects between folders](#)

To duplicate the folder structure

If you are adding multiple objects from a directory and its subdirectories, you are asked if you want to duplicate the existing folder hierarchy on the CMS.

1. In the "Specify Folder Hierarchy" dialog box, choose a folder hierarchy option.
 - To place all of the objects in a single folder, select **Put the files in the same location**.
 - To recreate all of the folders and subfolders on the CMS as they appear on your hard drive, select **Duplicate the folder hierarchy**. Choose the topmost folder that you want to include in the folder hierarchy.

2. Click **Next**.

The "Confirm Location" dialog box appears.

To move objects between folders

1. In the "Confirm Location" dialog box, move objects to folders by selecting each object, and then clicking **Move Up** or **Move Down**.



You can also add folders and object packages by selecting a parent folder and clicking the New Folder or New Object Package button.



To delete a folder or object package, select it and click the Delete button.



You can drag-and-drop objects to place them where you want, and you can right-click objects to rename them.

By default, the title of the objects are displayed. You can display the local file names of the objects by clicking the **Show file names** button.

2. Click **Next**.

The "Specify Categories" dialog box appears.

To add objects to a category

If you want to add the selected objects to a category, you can create or select a category on the host CMS. You can add objects to more than one category.

1. In the "Specify Categories" dialog box, select the category to which you want to assign the objects.

Click **+** to the left of the category to view the subcategories.

To add a new category to the CMS, select a category and then click New Category. The new category appears and can be renamed.



2. If you are adding more than one object, choose the object you want to add to the category from the **File** list.

Note:

Each object must be added to the category individually.

3. Click **Insert File**.



4. To delete a category or to remove an object from a category, select the item and click **Delete**.



Note:

From the wizard, you can delete only new categories. (New categories are green; existing categories are blue.)

5. Click **Next**.

The "Specify Schedule" dialog box appears.

To change scheduling options

The "Specify Schedule" dialog box allows you to schedule the objects you are adding to run at specific intervals.

Note:

This dialog box appears only for objects that can be scheduled.

1. In the "Specify Schedule" dialog box, select the object that you want to schedule.
2. Select one of three intervals:

- **Run once only**

Selecting the **Run once only** option provides two more sets of options:

- **when finished this wizard**

This option runs the object once when you finish adding it. The object is not run again until you reschedule it.

- **at the specified date and time**

This option runs the object once at a date and time you specify. The object is not run again until you reschedule it.

- **Let users update the object**

This option does not schedule the object. Instead, it leaves the task of scheduling up to the user.

- **Run on a recurring schedule**

Once you have selected this option, click the **Set Recurrence** button to set the scheduling options.

The "Pick a recurrence schedule" dialog box appears.

The options in this dialog box allow you to choose when and how often the object runs. Select the appropriate options and click **OK**.

3. Click **Next** after you have set the schedule for each object you are adding.

To refresh repository fields

The CMS database acts as a central repository in which shared elements such as text objects, bitmaps, custom functions, universes, and custom SQL commands are stored. You can choose to refresh the repository fields of an object if the object references the repository. To complete this task, the Publishing Wizard needs to connect to your CMS database from the local machine. For more details, see the *SAP BusinessObjects Enterprise Administrator's Guide*.

Note:

The "Specify Repository Refresh" dialog box appears only when you add report objects.

1. In the "Specify Repository Refresh" dialog box, select a report, and then select the **Use Object Repository when refreshing report** check box if you want to refresh it against the repository.

Tip:

Click the **Enable All** button if you want to refresh all of the objects that reference the repository; click the **Disable All** button if you want to refresh none of the objects.

2. Click **Next**.

To add objects with saved data

If you add a report that includes saved data, you are prompted by the "Specify Keep Saved Data" dialog box.

Note:

The "Specify Keep Saved Data" dialog box appears only when you add report objects.

1. In the "Specify Keep Saved Data" dialog box, select a report, and then select the **Keep saved data when publishing report** check box if you want to keep the report's saved data.

Tip:

Click the **Enable All** button if you want to keep the saved data for all of the reports; click the **Disable All** button if you do not want to keep saved data for any of the reports.

2. Click **Next**.

To select a program type

The "Program type" dialog box appears only when you add program objects.

1. In the "Program type" dialog box, select a program.
2. Choose one of the following program types:

- **Binary/Batch**

Binary/batch programs are executables, such as binary files, batch files, or shell scripts. They generally have file extensions such as .com, .exe, .bat, or .sh. You can publish any executable program that can be run from the command line on the machine where the Program Job Server is running.

- **Java**

You can publish any Java program to BusinessObjects Enterprise as a Java program object. They typically have a .jar file extension.

- **Script**

Script program objects are JScript and VBScript scripts.

3. After you specify the type of program that you are adding, click **Next**.

The "Program credentials" dialog box appears.

Related Topics

- [Program object management](#)

To specify program credentials

1. In the "Program Credentials" dialog box, select a program.
2. In the **User Name** and **Password** fields, specify the user credentials for the account that you want to use for the program to run.

The rights of the program are limited to those of the account with which it runs.

3. After you specify the user credentials for each program to use, click **Next**.
The "Change Default Values" dialog box appears.

To change the default values for an object

You can add objects without changing any of the default properties. However, if you use the default values, your object may not schedule properly if the database logon information is incorrect or if the parameter values are invalid.

1. Choose whether you want to change the default values for the object.
 - If you want to keep the default values:
 - a. Select **Publish without modifying properties**.
 - b. Click **Next** through the wizard's remaining dialog boxes.
 - If you want to change the default values, select **Review or modify properties**.

The "Review Object Properties" dialog box appears.

2. In the "Review Object Properties" dialog box, select the object that you want to modify.
3. Enter a new title or description.
4. If you are publishing a report object, select the **Generate thumbnail image** check box if you want users to see a thumbnail of the object before they open it.

Tip:

The **Generate thumbnail image** check box is available only if the object is a .rpt file and was saved appropriately. (To be able to display thumbnails for a report, open the report in Crystal Reports and, on the **File** menu,

click **Summary Info**. Select the **Save preview picture** option, and click **OK**. Preview the first page of the report and save your changes.)

5. Click **Next**.

The "Specify Database Credentials" dialog box appears if it is needed.

To enter database logon information

Note:

This option applies to Crystal reports only.

1. In the "Specify Database Credentials" dialog box, double-click the object, or click **+** to the left of the object to expose the database.
2. Select the database and change the logon information in the appropriate fields. If the database does not require a user name or password, leave the fields blank.

Note:

Enter user name and password information carefully. If it is entered incorrectly, the object cannot retrieve data from the database.

3. After you finish typing the logon information for each object, click **Next**.

The "Set Report Parameters" dialog box appears if it is needed.

To set parameters

Note:

This option applies to Crystal reports only.

Some objects contain parameters for data selection. Before these objects can be scheduled, you must set the parameters to determine the objects' default prompts.

1. In the "Set Report Parameters" dialog box, select the object that includes the prompts that you want to change.

The object's prompts and default values appear in a list on the right-hand side of the screen.

2. Click **Edit Prompt** to change the value of a prompt.

Depending on the type of parameter that you have chosen, different dialog boxes appear.

3. If you want to set the prompts to contain a null value (where possible), then click **Set Prompts to NULL**.
4. Click **Next** after you have finished editing the prompts for each object.

The "Specify Format" dialog box appears.

To set the schedule output format

Note:

This option applies to Crystal reports only.

You can choose an output format for each scheduled report that you add. For some of the formats, you can customize the schedule format options.

1. In the "Specify Format" dialog box, select the object that you want to set up to produce a different schedule output format.
2. Select a format from the list (Crystal report, Microsoft Excel, Microsoft Word, Adobe Acrobat, and so on).
3. Where applicable, customize the schedule format options.

For example, if you select Paginated Text, enter the number of lines per page.

4. Click **Next**.

To add extra files for programs

Some programs require access to other files in order to run.

1. Select a program.
2. Click **Add** to select the necessary file.
3. After you add all the necessary extra files for each program, click **Next**.

The "Command line for Program" dialog box appears.

To specify command line arguments

For each program, you can specify any command-line arguments that are supported by your program's command-line interface. They are passed directly to the command-line interface without parsing.

1. Select a program.
2. In the **Command line** area, type the command-line arguments for your program.

Note:

Use the same format you normally use at the command line.

3. After you specify all necessary command-line arguments for each program, click **Next**.

To finalize the objects to be added

After you provide the required information for the objects, the Publishing Wizard displays a list of all the objects that you chose to add.

1. Ensure that all of the objects that you want to add are on the list, and click **Next**.

The objects are added to the CMS, scheduled, and/or run as specified. Afterwards, you return to the final screen of the Publishing Wizard.

2. To view the details of an object, select it from the list.
3. Click **Finish** to close the wizard.

To add an object with the CMC

If you have administrative rights to BusinessObjects Enterprise, you can add objects over the Web from within the CMC. Use the CMC to add single objects or to perform administrative tasks remotely.

1. Go to the "Folders" management area of the CMC.
2. Browse for the folder that you want to add an object to and select it.
3. On the **Manage** menu, point to **Add** and click the appropriate option.

Option	Description
Crystal Report	Adds a Crystal report.
Program File	Adds a program object.
Local Document	Adds other types of objects.

A dialog box appears and lets you specify the properties of the object. This dialog box varies depending on the option you selected.

4. Specify the properties of the object.

Note:

The properties fields that appear vary according to the type of object that you chose to publish. The properties fields are summarized in "Object properties in the CMC".

5. If you want to assign the object to a category, select the category from the list.

6. Click **OK**.

The dialog box closes, and the CMC refreshes to display the object and the other contents of the folder.

If necessary, you can modify properties such as title, description, database logon information, scheduling information, user rights, and so on for the object after it is published to the CMC.

Table 25-1: Object properties in the CMC

Object type	Property	Notes
Crystal reports and other object types	Title	Enter the name of the object.
	Description	Enter a description for the object.
	Keywords	Enter keywords for the object.
	Filename	Enter the name of the object you want to add, or click Browse to find the object.
Crystal reports only	Keep saved data	Select this option if you want the report to keep its saved data.

Object type	Property	Notes
Program files only	Browse for an existing Program object	Enter the name of the program object you want to add, or click Browse to find the object.
	Program type	Click one of the options below Program type to define the type of program you are adding. The options are: <ul style="list-style-type: none"> • Executable (binary, batch, shell script) • Java • Script (VBScript, JavaScript)
Other object types only	File type	Select a file type from the File type list that matches the type of object you are adding.
	MIME	Specify the MIME extension for the object if needed.

Saving objects directly to the CMS

If you installed one of the Business Objects designer components, such as Crystal Reports, Designer, or Voyager, you can use the **Save As** command to add objects directly to BusinessObjects Enterprise from within the designer.

For example, after you design a report in Crystal Reports, on the **File** menu, click **Save As**. In the "Save As" dialog box, click **Enterprise**; then, when prompted, log on to the CMS. Specify the folder where you want to save the report, and click **Save**.

Desktop Intelligence documents can be published directly to the CMS using the **File > Export to Repository** command in the Desktop Intelligence Designer.

Web Intelligence documents can be published directly to the CMS using the **File > Export to CMS** command in Web Intelligence.

Note:

You can add Voyager workspaces to BusinessObjects Enterprise; however, you cannot set them to run on a recurring schedule.



Publishing and Publications



26

chapter



Overview

This section introduces you to the Publishing feature and publications. Most of the information in this section is related to the publisher's role.

As an administrator, you may be required to perform deployment configuration and troubleshooting tasks on behalf of publishers to optimize Publishing performance.

For more information about Publishing, refer to the *SAP BusinessObjects Enterprise Publisher's Guide* available online at http://support.businessobjects.com/documentation/product_guides/default.asp.

Note:

Publications and the Publishing feature are different from the Publishing Wizard. The Publishing feature uses publications to distribute personalized documents to a mass audience. The Publishing Wizard is a BusinessObjects Enterprise component that you use to add reports to the CMS.

Related Topics

- [Improving Publishing performance](#)

About Publishing

“Publishing” is the process of making documents such as Crystal reports, Web Intelligence documents, and Desktop Intelligence documents publicly available for mass consumption. The contents of these documents can be distributed automatically via email or FTP, saved to disk, or managed through the BusinessObjects Enterprise platform for web viewing, archiving, and retrieval, and automated through the use of scheduling. From within InfoView or the CMC, you can take documents and tailor them for different users or recipients; schedule a publication to run at specified intervals; and send it to a number of destinations, including recipients' Business Objects inboxes and email addresses.

What is a publication?

A “publication” is a collection of documents intended for distribution to a mass audience. Before the documents are distributed, the publisher defines the publication using a collection of metadata. This metadata includes the publication source, its recipients, and the personalization applied.

Publications can help you send information through your organization more efficiently:

- They allow you to easily distribute information to individuals or groups of users and personalize the information each user or group receives.
- They provide delivery of targeted business information to groups or individuals through a password-protected portal, across an intranet, an extranet, or the Internet.
- They minimize database access by eliminating the need for users to send process requests themselves.

You can create different types of publications based on Crystal reports, Desktop Intelligence documents, or Web Intelligence documents.

Publishing multiple documents

Publications are based on dynamic content documents and must include at least one Crystal report, Desktop Intelligence document, or Web Intelligence document. You can deliver multiple dynamic content documents and static documents as a single entity (for example, in a single email) in BusinessObjects Enterprise. You can also choose to zip the instances when they are delivered to recipients or, in the case of Crystal reports, to merge the instances into a single PDF with numbered pages.

If you design a publication with multiple documents in it, all dynamic content documents in that publication must be the same object type. For example, you can publish three Crystal reports in the same publication, but you cannot publish two Crystal reports and a Desktop Intelligence document.

A publication can also include static documents stored in the CMS repository such as the following:

- Microsoft Word/ Excel/ PowerPoint files

- Text files
- PDFs
- Agnostic documents

Publishing workflow

There are four categories of users for publications: document designers, publishers, administrators, and recipients.

Document designers do the following:

- Design documents (Crystal reports, Desktop Intelligence documents, or Web Intelligence documents) on which the publication is based.

For more information, see these guides:

- *Crystal Reports User's Guide*
- *SAP BusinessObjects Desktop Intelligence Online Help*
- *SAP BusinessObjects Web Intelligence Online Help*
- Design documents that are used as dynamic recipient sources.

For more information, see [Dynamic recipients](#).

- Add documents to the BusinessObjects Enterprise system.

Publishers use Publishing to:

- Create publications for distribution.

To create a publication, publishers follow a standard workflow:

- They locate the documents on which the publication will be based.
- They provide information to define the publication and personalize it for recipients.
- They schedule the publication to run.
- Select recipients for publications.
- Apply profiles to publications to tailor the type of information each user group will see.
- Redistribute instances of publications that have run successfully.

Administrators have the authority to:

- Create profiles.
- Manage mail server configuration.
- Configure external destinations such as local disk or an FTP server.

Recipients use “Publishing” to:

- Receive publications.
- Subscribe to and unsubscribe from publications.

Rights required for Publishing

Role	Task	Rights required
Document designer	Create the document on which the publication is based	None
Document designer	Add the document to the BusinessObjects Enterprise system	<ul style="list-style-type: none">• View and Add rights on the folder or category to which the document will be added
Document designer	Create a document to be used as a dynamic recipient source	<ul style="list-style-type: none">• View and Add rights on the folder or category to which the document will be added
Publisher	Create a publication	<ul style="list-style-type: none">• Add right on the folder where the publication is saved• View right on users and groups intended as recipients• View right on the profile that is used for personalization• View right on documents and other documents for the publications• Schedule rights on the documents• Subscribe to Publications rights on the Enterprise recipients

Role	Task	Rights required
Publisher	Schedule a publication	<p>Note: It is recommended that only the publisher has the rights listed below.</p> <p>Tip: When setting rights on the publication, remember to set them in the General tab.</p> <ul style="list-style-type: none"> • View, Schedule, Add, and Modify Security rights on the publication • Delete Instance right on the publication • View right on users and groups intended as recipients • View right on the profile that is used for personalization • View and Schedule rights on the documents • View and Refresh rights on the dynamic recipient source • View and Refresh rights on the document on which a delivery rule is set • Data Access right on any universes used by the publication's objects • Data Access right on any universe connections used • Add and View rights on recipients' SAP Business Objects inboxes (when you schedule to inboxes) • Subscribe to Publications rights on the recipients • Print right on Crystal report source documents if the publisher wants to print publication instances • Schedule on behalf of other users right on Enterprise recipients (if you use One database fetch per recipient)

Role	Task	Rights required
Publisher	Retry a failed publication instance	<ul style="list-style-type: none"> • Same rights required to schedule a publication • Edit right on the publication instance
Publisher	Redistribute a publication instance	<ul style="list-style-type: none"> • View, Schedule, Add, and Modify Security rights on the publication • Add and View rights on recipients' Business Objects inboxes • View Instance and Edit rights on the publication instance
Recipient	View a publication	<ul style="list-style-type: none"> • View right on the publication • View Instance right on the publication <p>Note: You need these rights to view a publication object in the BusinessObjects Enterprise system. You do not need these rights to see content sent to a Business Objects inbox.</p>
Recipient	Subscribe to or unsubscribe from a publication	<ul style="list-style-type: none"> • View right on the publication • Subscribe to Publications rights on the Enterprise recipients

Publication concepts

Report bursting

During Publishing, the data in documents is refreshed against data sources and personalized before the publication is delivered to recipients. This combined process is known as “report bursting”. Depending on the size of the publication and how many recipients it is intended for, you have several report bursting methods to choose from:

- **One database fetch for all recipients**

When you use this report bursting method, the data is refreshed once for each document in the publication, and the documents are personalized and delivered to each recipient. This report bursting method uses the data source logon credentials of the publisher to refresh data.

This is the default option for Desktop Intelligence and Web Intelligence document publications. It is also the recommended option if you want to minimize the impact of Publishing on your database. This option is secure only when the source documents are delivered as static documents. For example, a recipient who receives a Desktop Intelligence document in its original format can modify the document and view the data associated with other recipients. However, if the Desktop Intelligence document was delivered as a PDF, the data would be secure.

Note:

- This option is secure for most Crystal reports regardless of whether the Crystal reports are delivered in their original format.
- The performance of this option varies depending on the number of recipients.
- **One database fetch for each batch of recipients**

When you use this report bursting method, the publication is refreshed, personalized, and delivered to recipients in batches. This report bursting method uses the data source logon credentials of the publisher to refresh data. The batches are based on the personalization values you specified for the recipients. The batch size varies depending on the specified personalization value and is non-configurable.

This is the default option for Crystal report publications. It is also the recommended option for high-volume scenarios. With this option, you can process batches concurrently on different servers, which can greatly decrease the processing load and time required for large publications. This option is also recommended for Desktop Intelligence document publications if you want to maximize security for publication instances.

Note:

This option is unavailable for Web Intelligence documents.

- **One database fetch per recipient**

The data in a document is refreshed for every recipient. For example, if there are five recipients for a publication, the publication is refreshed five

times. This report bursting method uses the data source logon credentials of the recipient to refresh data.

This option is recommended if you want to maximize security for delivered publications.

Note:

Crystal reports that are based on universes or Business Views support **One database fetch per recipient** only to maximize security.

Delivery rules

Note:

This feature is unavailable for Web Intelligence documents.

“Delivery rules” affect how documents in publications are processed and distributed. When you set delivery rules on documents, you indicate that the publication will be delivered to recipients only if the content in the documents meets certain conditions. There are two types of delivery rules:

- Recipient delivery rule

If the data in the recipient's instance meets the delivery rule, the instance is delivered to the recipient.

- Global delivery rule

If the data in a designated document meets the delivery rule, the publication is delivered to all recipients.

Note:

The designated document for a global delivery rule can be different from the document or documents used in a publication. For example, you can set a global delivery rule on a Desktop Intelligence document used as a dynamic recipient source instead of a Desktop Intelligence document in the publication.

If a publication has recipient and global delivery rules, the global delivery rule is evaluated first to determine whether the publication will be processed. If the publication meets the global delivery rule, the system then evaluates the recipient delivery rules to determine which instances to process and distribute for each recipient.

How you set delivery rules depends on the document type that you want to publish. For Crystal reports, you specify a delivery rule based on a named alert that the report designer creates in the Crystal report. For Desktop Intelligence documents, you specify a formula expression. You can also set a delivery rule based on whether the personalized publication contains any data.

The diagram “Global delivery rule met” illustrates how an alert-based global delivery rule works. Here the global delivery rule is set on a document in the publication. The Crystal report has a Revenue alert for values greater than 100,000. The publisher creates a global delivery rule based on the Revenue alert so that the Crystal report is only delivered to all recipients if revenue exceeds 100,000. In this case the delivery rule is met, so the Crystal report is delivered.

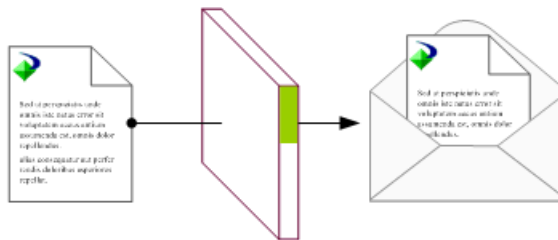


Figure 26-1: Global delivery rule met

The diagram “Recipient delivery rule unmet” illustrates how a recipient delivery rule works. The publisher sets a recipient delivery rule for the Crystal report so that the report is delivered to recipients only if the report contains data for that recipient. When the report is personalized for each recipient, Green Recipient does not have data in the Crystal report. This means that only Blue Recipient and Orange Recipient receive the publication.

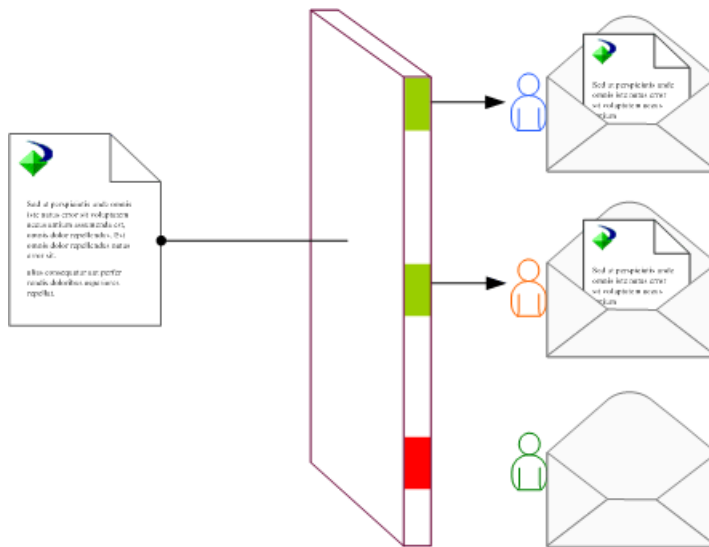


Figure 26-2: Recipient delivery rule unmet

For publications that contain multiple documents and objects, each document can have its own recipient delivery rule. When you do this, you have the following options for processing and delivery:

- If a document in the publication fails to meet its recipient delivery rule for a recipient, the entire publication will not be delivered for that recipient.
- If a document in the publication fails to meet its recipient delivery rule for a recipient, that document will not be delivered, but all other documents in the publication will be delivered for that recipient.

Delivery rules are useful because they allow publications intended for a large number of recipients to be processed and distributed more efficiently.

Consider a situation in which a publisher at an insurance company creates a publication for its clients that contains the following objects:

- An insurance bill (personalized Crystal report).
- A monthly statement (personalized Crystal report).
- A payment methods brochure (PDF).

In the insurance bill, there is an Amount Due alert for values greater than zero. The publisher creates an Amount Due recipient delivery rule for the insurance bill so that the insurance bill is published and distributed only if a client owes the insurance company a payment. The publisher also specifies that the entire publication will not publish if the insurance bill fails to meet the delivery rule because he does not want clients to receive a monthly

statement and a brochure when they do not have to pay a bill. When the publication is run, the publication is processed and distributed to clients who owe payments only.

Note:

If a Crystal reports publication is scheduled to print when the publication runs, the print job occurs regardless of whether a document in a publication fails to meet a delivery rule and is not delivered to a recipient. This is because print jobs are processed during personalization, and delivery rules are applied to publications after personalization.

Dynamic recipients

“Dynamic recipients” are publication recipients who exist outside of the BusinessObjects Enterprise system. Dynamic recipients already have user information in an external data source, such as a database or an LDAP or AD directory, but do not have user accounts in BusinessObjects Enterprise.

To distribute a publication to dynamic recipients, you use a “dynamic recipient source”. A dynamic recipient source is a document or custom data provider that provides information about publication recipients outside of the BusinessObjects Enterprise system. Dynamic recipient sources allow you to easily maintain information for dynamic recipients by linking directly to the external data source and retrieving the most recent data. They also decrease administrative costs because you do not have to create BusinessObjects Enterprise user accounts for dynamic recipients before you distribute publications to them.

Consider a situation in which a billing company distributes bills to customers who are not BusinessObjects Enterprise users. The customer information already exists in an external database. The publisher creates a document based on the external database and uses the document as a dynamic recipient source for a publication. The customers receive the billing publication, and the dynamic recipient source allows the publisher and the system administrator to maintain up-to-date contact information.

You can do the following with a dynamic recipient source:

- Deliver a single publication to dynamic recipients and BusinessObjects Enterprise users simultaneously.

Note:

- Only one dynamic recipient source can be used for each publication.
- Dynamic recipients cannot unsubscribe themselves automatically from a publication.
- Preview the dynamic recipients list when you create a publication.
- Specify whether you want to deliver the publication to all dynamic recipients, or to include or exclude certain dynamic recipients.
- Deliver publications to external destinations such as email or an FTP server.

Note:

Business Objects inboxes are invalid destinations for dynamic recipients because they do not have BusinessObjects Enterprise user accounts.

To use a dynamic recipient source, you specify a column for each of the following values:

- Recipient ID (required)
- Full name of recipient
- Email address

The recipient ID column determines the number of dynamic recipients who will receive the publication. It is recommended that you sort the dynamic recipient source according to recipient ID.

For information about creating a dynamic recipient source in Crystal Reports, see the *Crystal Reports User's Guide*. For information about creating a custom-coded dynamic recipient source, see the *SAP BusinessObjects Enterprise Java SDK Developer Guide*.

Related Topics

- devlibrary.businessobjects.com

Destinations

Destinations are locations that you deliver publications to. A destination can be the BusinessObjects Enterprise location in which a publication is stored, an Business Objects inbox, a email address, an FTP server, or a directory on the file system. You can specify multiple destinations for a publication.

If you are publishing multiple Crystal reports, you can also merge them into a single PDF on a per destination basis.

If you want to publish a publication as a single ZIP file, you can choose to zip or unzip the instances on a per destination basis (for example, zip the instances for email recipients and leave them unzipped for Business Objects inboxes).

Related Topics

- [*Possible destinations*](#)

Possible destinations

Destination	Description
Default Enterprise location	<p>The publication is accessible from the folder in which it was created. For the default destination, you have these options:</p> <ul style="list-style-type: none">• Merge all PDF documents (Crystal reports only).• Package the publication as a ZIP file. <p>Note: If you distribute a publication to the default location or a shortcut to a recipient's Business Objects inbox, you must select a folder that is accessible to all recipients as the publication's location.</p>
Business Objects inbox	<p>The publication is sent to the recipient's Business Objects inbox. For the Business Objects inbox destination, you have these choices:</p> <ul style="list-style-type: none">• Deliver objects to each user.• Have the target name automatically generated, to enter a specific name for it, or to choose from a list of placeholders.• Have the publication sent as a shortcut or as a copy.• Merge all PDF documents (Crystal reports only).• Package the publication as a ZIP file.
Email	

Destination	Description
	<p>The publication is sent to recipients via email. For email recipients, it is recommended that you complete the From field. If you do not complete the From field, BusinessObjects Enterprise uses the email address associated with the publisher's account. If the publisher's account has no email address, BusinessObjects Enterprise uses the Destination Job Server's settings.</p> <p>Note: If there is no From value provided by the From field, the publisher's account, or the Destination Job Server, the publication will fail.</p> <p>You also have these choices:</p> <ul style="list-style-type: none"> • Deliver objects to each user. • Complete the To field or enter a placeholder for the email address. • Complete the Cc field. • Enter the subject or select a placeholder to use for this field. • Enter text in the Message field to be delivered with your publication. You can also choose from a list of placeholders to use in the Message field and embed dynamic content document content in the body of the email. • Attach source document instances to the email. • Have the attachment name automatically generated, to enter a specific name for it, or to choose from a list of placeholders. • Merge all PDF documents (Crystal reports only). • Package the publication as a ZIP file. <p>Note:</p> <ul style="list-style-type: none"> • Before you use this destination, ensure that your email settings are configured properly on the Destination Job Server. • If you are sending publications to recipients via email, ensure the placeholder %SI_EMAIL_ADDRESS% is in the To field and Deliver objects to each user is selected.
FTP server	

Destination	Description
	<p>For FTP server, complete the Host field. If you do not complete the Host field, the option configured for the Destination Job Server will be used. You also have these choices:</p> <ul style="list-style-type: none">• Specify a port number, a user name and password, and an account.• Enter a directory name.• Have the file name automatically generated, to enter a specific name for it, or to choose from a list of placeholders. If Specific name is selected, you can also choose to add a file extension.• Merge all PDF documents (Crystal reports only).• Package the publication as a ZIP file.
Local disk	<p>If you choose local disk as the destination, you must enter the directory for your publication. You also have these choices:</p> <ul style="list-style-type: none">• Deliver objects to each user.• Have the file name automatically generated, to enter a specific name for it, or to choose from a list of placeholders. If you select a specific name, you can also choose to add a file extension.• Enter a user name and password to access the file location.• Merge all PDF documents (Crystal reports only).• Package the publication as a ZIP file.

Note:

- **Deliver objects to each user** 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 and thus receive the same data in their publication instances. If you clear **Deliver objects to each user**, one publication instance is generated and delivered to all three recipients. If you select **Deliver objects to each user**, the same publication instance is delivered three times (once for each recipient). Additionally, if you are sending the publication to an FTP server or local disk destination and some recipients share identical personalization values, you can clear **Deliver objects to each user** to decrease overall processing time.
- If you clear **Deliver objects to each user**, any placeholders that you use when you configure your destinations will contain the publisher's information and not the recipient's.

Formats

Formats define the file types that a publication's documents will be published in. A single document can be published in multiple formats, and these instances can be delivered to multiple destinations. For publications with multiple documents, you can specify a different format for each. For publications that contain Desktop Intelligence or Web Intelligence documents, you can publish the whole document or a report tab within the document to different formats.

Any formats you choose for a document apply to all recipients of the publication. For example, you cannot publish a document as a Microsoft Excel file for one recipient and as a PDF for another. If you want the recipients to receive instances in those formats, each recipient will receive a Microsoft Excel file and a PDF.

Possible formats

Document type	Format	Description
All document types	mHTML	<p>This option publishes the document in mHTML format. You can also embed a document's content as mHTML in an email:</p> <ul style="list-style-type: none">• For Crystal reports, you can embed the content of one report in an email.• For Desktop Intelligence documents, you can embed the content of one report tab or all report tabs from a single document in an email.• For Web Intelligence documents, you can embed the content of one report tab in an email. <p>When mHTML is selected, the output will reflect the order in which the source documents are arranged on the document selection screen. For example, the documents displayed at the top of the screen will appear at the top of the email.</p>
	PDF (.pdf)	<p>This option publishes a document as a static PDF.</p> <p>Note: When this is used together with the PDF merging option, the output will reflect the order in which the source documents are arranged on the document selection screen. For example, the documents displayed at the top of the screen will appear at the top of the merged PDF.</p>
	Microsoft Excel file (.xls)	<p>This option publishes a document as a Microsoft Excel file and preserves as much of the original format of the document as possible.</p>

Document type	Format	Description
Crystal reports	Data only Microsoft Excel file (.xls)	This option publishes a Crystal report as a Microsoft Excel file that contains data only.
	XML	This option publishes a Crystal report in XML format.
	Crystal report (.rpt)	This option publishes a Crystal report in its original format.
	Microsoft Word file (.doc)	This option publishes a Crystal report as a Microsoft Word file and preserves the original formatting of the Crystal report. This option is recommended if you expect recipients to view the publication without making many changes to it.
	Editable Microsoft Word file (.rtf)	This option publishes a Crystal report as a Microsoft Word file that you can edit more easily. This option is recommended if you expect recipients to view the publication and edit its content.
	Rich text (.rtf)	This option publishes a Crystal report in rich text format.
	Plain text (.txt)	This option publishes a Crystal report in plain text format.
	Paginated text (.txt)	This option publishes a Crystal report in plain text format and paginates the content of the publication.
	Tab-separated text (.txt)	This option publishes a Crystal report in plain text format and separates the content in each column using tabs.
	Character-separated values (.csv)	This option publishes a Crystal report as a character-separated values file.

Document type	Format	Description
Desktop Intelligence documents	Desktop Intelligence document (.rep)	This option publishes a Desktop Intelligence document in its original format.
	Rich text (.rtf)	This option publishes a Desktop Intelligence document in rich text format.
	Plain text (.txt)	This option publishes a Desktop Intelligence document in plain text format.
Web Intelligence documents	Web Intelligence document (.wid)	This option publishes a Web Intelligence document in its original format.

Personalization

“Personalization” is the process of filtering data in source documents so that only relevant data is displayed for publication recipients. Personalization alters the view of the data, but it does not necessarily change or secure the data being queried from the data source.

The diagram “Personalization” illustrates how personalization works. An unpersonalized report contains data types 1, 2, and 3. When the personalization is applied to the report, users only receive the data that is relevant to them: User 2 only receives data type 2, User 1 only receives data type 1, and User 3 only receives data type 3.

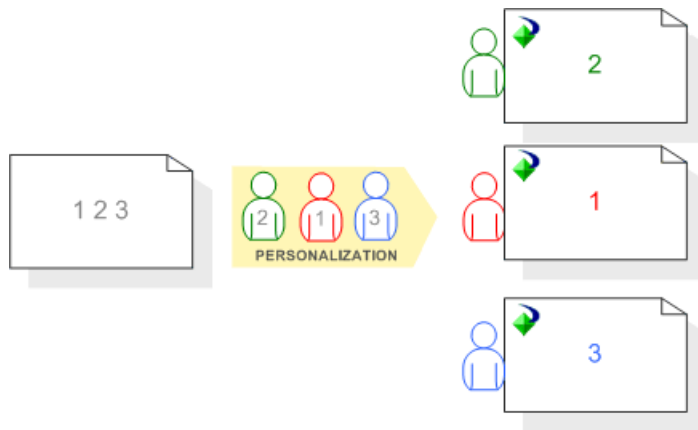


Figure 26-3: Personalization

To personalize source documents for recipients, you can do the following:

- If the recipients are Enterprise recipients, you can apply a profile when you design the publication.
- If the recipients are dynamic recipients, you can map a data field or column in the source document to data in the dynamic recipient source. For example, you can map a Customer ID field in a source document to the Recipient ID field in the dynamic recipient source.

For Crystal report publications, you specify the personalization that is used in the "Personalization" section. If no personalization is specified and the report contains parameters, the Publishing feature uses the personalized parameter values; if these personalized parameter values do not exist, the Publishing feature uses the default parameter values. If none of these settings exist, personalization does not occur for a recipient.

Related Topics

- [How profiles work](#)

Subscription

A "subscription" allows users who were not specified as recipients of a publication to receive publication instances when the publication runs. Users can subscribe to a publication if they want to view the latest instance, or they

can unsubscribe from a publication they no longer want to receive. If a user has the appropriate rights, the user can also subscribe and unsubscribe other users.

To subscribe to and unsubscribe from a publication, a user must have the following:

- Appropriate rights, including:
 - View right on the publication.
 - Subscribe to publications right on user accounts for Enterprise recipients.
- Access to InfoView or the CMC.
- A BusinessObjects Enterprise account.

Note:

Dynamic recipients cannot subscribe and unsubscribe themselves automatically.

To create a new publication in the CMC

This task lets you access the Publishing feature in the CMC and begin creating a publication.

1. Go to the "Folders" area of the CMC.
2. In the Tree panel, browse for the folder in which you want to create the publication.
3. Select the folder so that its contents are displayed in the Details panel.
4. Click **Manage > New > Publication**.

The **New Publication** page appears.

On the **New Publication** page, you can specify all the information required for your publication, including source documents, recipients, delivery formats and destinations, and how those documents are personalized.

To create a new publication in InfoView

This task lets you access the Publishing feature in InfoView and begin creating a publication.

1. Click **Document List**.

2. In the Tree panel, browse for the folder in which you want to create the publication.
3. Select the folder so that its contents are displayed in the Details panel.
4. Click **New > Publication**.

The **New Publication** page appears.

On the **New Publication** page, you can specify all the information required for your publication, including source documents, recipients, delivery formats and destinations, and how those documents are personalized.



Managing Profiles

27

chapter

How profiles work

Profiles are objects in the BusinessObjects Enterprise system that let you classify users and groups. They work in conjunction with publications to personalize the content that users see. Profiles link users and groups to profile values, which are values used to personalize data within a report. Profiles also use profile targets, which describe how a profile is applied to a report. By assigning different profile values, the data within a report can be tailored to specific users or groups. Many different personalized versions of the report are then delivered to your users.

Often profiles reflect the roles of users and groups in an organizational structure. For example, you could have a Department profile that includes all employees in an organization. The users and groups each have profile values that reflect their roles in the organization (for example, "Finance", "Sales", and "Marketing"). When a publisher applies the Department profile to a publication, the employees receive data that is relevant to their department.

Profiles do not control users' access to data. Profiles are used to refine or filter a document's content. When you use profiles to display a subset of the data to a user, it is not the same as restricting the user from seeing that data. If users have the appropriate rights and access to the document in its original format, they may still see the complete data for the document by viewing it in InfoView or the CMC. Profiles filter the view of the data; they do not change or secure the data being queried from the data source.

Note:

Publications and the Publishing feature are different from the Publishing Wizard. The Publishing feature uses publications to distribute personalized documents to a mass audience. The Publishing Wizard is a BusinessObjects Enterprise component that you use to add reports to the CMS.

Related Topics

- [How rights work in BusinessObjects Enterprise](#)

Profiles and the Publishing workflow

The administrator and the publisher do different tasks to ensure that a profile can be used to personalize content during Publishing.

First, the administrator does the following in the "Profiles" management area of the CMC:

1. creates a profile
2. adds users and groups to the profile
3. assigns profile values to each user and group for that profile
4. specifies a global profile target if necessary

During Publishing, the publisher does the following to use the profile to personalize a publication:

1. adds users and groups to a publication as recipients
2. specifies a local profile target for the profile to filter (for example, a field in a Crystal report)
3. specifies the profile or profiles that will be used for personalization

For more information about personalization and Publishing, see the *SAP BusinessObjects Enterprise Publisher's Guide*.

To create a profile

1. Go to the "Profiles" management area of the CMC.
2. Click **Manage > New > New Profile**.
The "Create New Profiles" dialog box appears.
3. Type a name for the profile in the **Title** field.
4. Complete the **Description** field.
5. Click **OK**.

You can now use the profile to perform the following tasks:

- Use global profile targets to personalize the data on the universe and class level.
- Use profile values to personalize the data on the user and group level.
- Set rights on profiles.

Related Topics

- [To specify a global profile target](#)
- [To specify a profile value](#)
- [Specifying profile rights](#)

Profile targets and profile values

To use a profile to personalize a publication, you must set profile values and profile targets for the profile.

What are profile targets?

Profile targets are data sources that profile values filter and interact with to provide personalized publications. There are two types of profile targets:

- Local profile target

A local profile target can be a variable in a Desktop Intelligence document or Web Intelligence document, or a field or parameter in a Crystal report. When you use a local profile target, the source document that contains the local profile target is filtered for the publication recipients.

- Global profile target

A global profile target can be a universe. You must also specify an object within that universe. This type of profile target can filter all source documents that use the universe.

Note:

You can use global profile targets for publications that contain Desktop Intelligence and Web Intelligence documents. You cannot use global profile targets with Crystal reports.

What are profile values?

Profile values are attributes detailed to specific users or groups when you assign these users and groups to a profile. When a profile is applied to a publication, the users and groups assigned to that profile receive versions of the publication that are filtered according to the profile values set for them.

Note:

If you assign profile values to both users and groups, note that inheritance works the same way for profiles as it does for security settings. For more information, see [Inheritance](#).

Why are profile targets and profile values useful?

Profile targets and profile values enable a profile to personalize a publication for recipients. The users and groups specified for a profile receive filtered versions of the same publication that only display the data most relevant to them.

Consider a situation where a global sales report is distributed to a company's regional sales teams in North America, South America, Europe, and Asia. Each regional sales team only wants to view the data that is specific to their region. The administrator creates a Regional Sales profile and adds each regional sales team to the profile as a group. The administrator assigns each regional sales team a corresponding profile value (for example, the North America Sales group is assigned "North America"). During Publishing, the publisher uses the Region field in the global sales report as a local profile target, and applies the profile to the report. The global sales report is filtered according to the profile values set for each regional sales team. When the global sales report is distributed, each regional sales team receives a personalized version that only displays regional sales data.

To specify a global profile target

This task lets you specify a global profile target for a profile. Local profile targets are specified by the publisher during the Publishing process.

1. In the "Profiles" area of the CMC, select the profile that you want to specify a profile target for.
2. Click **Actions > Profile Targets**.
The "Profile Targets" dialog box appears.
3. Click **Add**.
4. Select a universe from the **Universe Name** list.
5. Enter a class name in the **Class Name** field, or click **Select object from the universe**.
6. Enter a variable name in the **Variable Name** field, or click **Select object from the universe**.

7. Click **OK**.

Specifying profile values

You can use static values, expressions, or variables as profile values.

Static values are the most common profile value type and can be used to filter any source document type. You can also enter multiple static values for a user or group for one profile. For example, a manager interested in receiving data from several departments can have “Production”, “Design”, and “Marketing” as static profile values for a Department profile.

Expressions use syntax that is specific to certain source document types. You can use Crystal Reports, Web Intelligence, and Desktop Intelligence expressions to perform more complex personalization and filtering. Expressions are useful if you want to filter a range of values, or a range of values greater than or less than a given value, for a user.

If you want to use user information as profile values, you can use variables for user names, full names, and email addresses. These variables are mapped to user information and act as placeholders. When you apply the profile to a publication, the system retrieves the most recent information for users.

Profile value variables are useful because they decrease administrative costs and possible errors associated with entering information manually. Consider a situation where an administrator maps an AD user to the system and adds the user to two profiles. Instead of entering the information manually for each profile value and possibly making typographical errors, the administrator can specify which variables to use for the user's data.

For third-party users, if the user's information changes in an external system, the data in the BusinessObjects Enterprise system can be updated to reflect those changes when a publication is run.

Tip:

If you have a third-party user account with data that should not be overwritten by user attributes in an external directory, open the “Properties” dialog box for the user object and clear the **Import full name and email address** check box.

The following table summarizes the variables that can be used for the externalization of profiles.

Variable	Description
<i>Title</i>	This variable is associated with the user's account name.
<i>User's full name</i>	This variable is associated with the user's full name.
<i>E-mail address</i>	This variable is associated with the user's email address.

Tip:

These variables can also be used for groups. You can map the *E-mail address* variable to a common email address for the entire group. When you do this, the system resolves the variable and retrieves individual email addresses for each member of the group.

Note:

- Static-value profile values can filter string fields in source documents only. If you map the incorrect type of field to the profile, personalization will fail.
- For Desktop Intelligence documents, expression profile values are only compatible with the report bursting method **One database fetch for all recipients**.

To specify a profile value

This task lets you specify a profile value for a user or group.

1. In the "Profiles" area of the CMC, select a profile.
2. Click **Actions > Profile Values**.
The "Profile Values" dialog box appears.
3. Click **Add**.
4. Click **Choose**.
5. Select a user or group or multiple users or groups, and click **>** to move them into the list on the right side.
6. Click **OK**.
7. Enter a profile value for the selected user or group or multiple users or groups.

You can use several different types of profile values. You can enter a static profile value or an expression. You can also specify variable profile values for third-party users and groups mapped to the system.

- If you want to use a value:

- a. Click **Value**.
- b. Enter a value in the **New Value** field.
- c. Click **Add**.

Tip:

You can add multiple static values for a user or group. Repeat steps 1-3 for each static value that you want to add.

- If you want to use a filter expression:
 - a. Click **Filter Expression**.
 - b. Depending on the type of expression you want to use, enter an expression in the **Desktop Intelligence expression** field, the **Web Intelligence formula expression** field, or the **Crystal Reports expression** field.

Note:

To use a Web Intelligence expression, you must first specify a global profile target for the profile.

Tip:

If you want to apply the profile to multiple document types, you can enter filter expressions in all three fields.

8. Click **OK**.

Related Topics

- [To use variables as profile values](#)

To use variables as profile values

This task lets you specify variable profile values for users when you add them to a profile. You can specify variable profile values for the user's full name, account name, or email address.

1. In the "Profiles" area of the CMC, select the profile that you want to add the user or group to.
2. Click **Actions > Profile Values**.
The "Profile Values" dialog box appears.
3. Click **Add**.
4. Click **Choose**.

5. Select the user or group from the list on the left, and click > to move the user or group to the list on the right.
6. Click **OK**.
7. Click **Value**.
8. Select a placeholder variable from the **Add placeholder** list, and click **Add**.

You can select a placeholder for the user's user name, full name, or email address.

The placeholder appears in the **Existing values** field.

9. 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.

Resolving conflicts between profiles

You may encounter conflicts between profiles when users and groups have been assigned multiple profiles through inheritance. If a document is delivered to a user that has two profiles that conflict, the difference must be resolved.

For example, Tony is a product manager in the Mexico office. He is assigned a profile called Region that personalizes his documents to show only data from Mexico. He is also assigned a different Management profile that personalizes the data to display data for product managers.

If a document uses both of these profiles, which data will Tony see? According to one profile, he'll see data for Mexico. According to the other profile, he should see only data for product managers.

BusinessObjects Enterprise can resolve this conflict in two ways:

- Do not merge

BusinessObjects Enterprise determines the different possible views of a publication that could be delivered and produces a unique view for each case. In the example, Tony would receive one publication personalized to show data for Mexico, and another publication that shows product manager data.

- Merge

With this setting, BusinessObjects Enterprise again determines the different possible views of the data, but this time the non-conflicting profiles are merged. This type of profile resolution is designed for role-based security. In the example, Tony would receive a single publication personalized to show data for Mexican product managers.

You can specify the Profile Resolution settings when you define your publications. For more information, see the *SAP BusinessObjects Enterprise Publisher's Guide*.

Note:

This “do not merge/merge” scenario applies to inherited profile values only. If a user is assigned two profile values explicitly, the publication instances are always merged.

Conflicts between profile values

Conflicts between profile values can arise when a user inherits two contradictory profile values as a result of group membership. In general, explicitly assigned profile values override profile values inherited from group membership. A profile value assigned to a user or a subgroup overrides the profile value inherited from group membership.

For example, David belongs to the North America Sales and Canada Sales groups. The Canada Sales group is a subgroup of the North America Sales group. These groups are both added to the Region profile. From the North America Sales group, David inherits a Region profile value of “North America”, and from the Canada Sales group, David inherits a Region profile value of “Canada”. In this case, the profile value that is assigned to the subgroup overrides the profile value that is assigned to the group, and David receives a publication with data for Canada.

Conflicts between profile values can also arise when a user is explicitly assigned a profile value that contradicts a profile value inherited from group membership. For example, Paula belongs to the North America Sales group, which has a Region profile value of “North America”. The administrator also assigns Paula a Region profile value of “Spain”. In this case, the profile value that is assigned to the member overrides the profile value that is inherited from the group, and Paula receives a publication with data for Spain.

However, sometimes a user can inherit different profile values from two different groups for one profile. Both groups are hierarchically equal; one group is not a subgroup of the other group, so one profile value does not override the other. In this case, both profile values are valid and the user receives a publication instance for each profile value.

As a result of this profile value conflict, sometimes duplicate report instances are included in different publication instances and sent to the same user. For example, Sandra is a manager in two North America offices and receives a publication via email that contains two reports. Report 1 is personalized using the Region profile, for which Sandra inherits the conflicting profile values “USA” and “Canada” from group membership. Report 2 is personalized using the Role profile, for which Sandra inherits the profile value “Manager”. If there is no profile value conflict, after personalization, Sandra receives one email with a merged Report 1 instance (USA and Canada data) and a Report 2 instance (Manager data). Instead, Sandra receives two emails: one email includes a Report 1 USA instance, the other email includes a Report 1 Canada instance, and both emails have the same Report 2 Manager instance.

Tip:

To avoid profile value conflicts that result in duplicate publication instances being sent, when possible, explicitly assign profile values to users instead of allowing users to inherit profile values from group membership.

Specifying profile rights

You can grant or deny users and groups access to profiles. Depending on how you organize your profiles, you may have specific profiles that you want to be available only for certain employees or departments.

Users with access to the CMC will only be able to see profiles they have the rights to see, so you can use rights to hide profiles that aren't applicable to a particular group. For example, by granting only the ITAdmin group access to IT-related profiles, those profiles won't appear for a user from the HRAdmin group; this makes the profile list easier for the HRAdmin group to navigate.

Related Topics

- *To assign principals to an access control list for an object*



Content Search

28

chapter



This section of the *BusinessObjects Enterprise Administrator's Guide* is for administrators of BusinessObjects Enterprise who want to use Content Search in their deployment. This section includes information on:

- Content Search overview
- Content Search administration

For information on how to conduct content searches in InfoView, see the *BusinessObjects Enterprise InfoView User's Guide*.

Content Search overview

Content Search is an optimized search tool that enables InfoView users to search within the content of objects managed by BusinessObjects Enterprise. It refines the search results by grouping them into categories of similar object types, and ranking them in order of their relevance to the search term.

Only reports to which a user has view rights will appear in the InfoView search results

Users conduct Content Searches by using techniques similar to those used in other search engines. These techniques are summarized in the *BusinessObjects Enterprise InfoView User's Guide*.

Searchable document types

Most content published to BusinessObjects Enterprise is searchable with Content Search. The following table summarizes object types the feature supports.

Object type	What gets searched
Crystal Reports	Title, description, selection formula, saved data, text fields in any section, parameter values, and sub-reports.
Web Intelligence and Desktop Intelligence documents	<p>Title, description, name of the Universe filters used in the report, constants in the filter condition locally defined in the report, name of the Universe measures used in the report, name of the Universe objects used in the report, data in record set, and static text in cells.</p> <p>Both reports with and without saved data are searchable.</p>
Microsoft Excel documents	<p>Data in all non-empty cells, fields on the Summary page of the document properties (title, subject, author, manager, company, category, keywords and comments), and text in document headers and footers.</p> <p>For cells that use calculation or formula, the value after the evaluation is searchable. For number or date/time values, the raw data is searchable.</p>
Word documents	Text in all paragraphs and tables, fields on the Summary page of the document properties (title, subject, author, manager, company, category, keywords and comments), text in document headers and footers, and numerical text.
RTF, PDF, and TXT Files	All text in these files is searchable.

Note:

Search for the following objects remains unchanged. Users can search for

the keyword, title, or description of these objects:

- Voyager workspace
- Hyperlink
- Program
- Object package
- Publication
- My InfoView page
- EPM dashboard
- EPM analytics

Because object packages and publications have objects within them, Content Search interacts with them in a slightly different way. For the object package or publication itself, the title, description, and keywords are indexed and searchable. However, the reports inside the package or publication are indexed as they would be if they were independent objects. When a match to an object contained in an object package or publication is found, the matched object is displayed as a search result and the object package or publication is displayed as part of the folder path for the object.

Search syntax and interpretation

Search input syntax is interpreted in much the same way as major search engines interpret syntax, so that Content Search will be easy to use. How to use search input syntax for Content Search is described in the Content Search section of the *SAP BusinessObjects Enterprise InfoView User's Guide*.

The language that you choose to optimize Content Search for affects three areas of search syntax and interpretation: stop words, stemming, and tokenization.

Stop words are words that are used so often in a language that including them in a search input will almost always result in undesirable search results. Content Search ignores these words in the search input, unless the word is preceded by “+”, which explicitly includes the word. Because stop words are different for every language, Content Search will only recognize stop words

for the language it has been optimized for. The following languages support stop words in Content Search:

- English
- French
- German
- Italian
- Spanish
- Dutch
- Swedish
- Portuguese
- Russian

The following languages do not support stop words in Content Search:

- Japanese
- Traditional Chinese
- Simplified Chinese
- Korean
- Polish

The spelling of a word can vary between tenses, parts of speech, and if a word is made plural. Stemming is the process of recognizing and searching for or indexing the root word, so that matches will still be returned across different forms of the same word. Stemming is applied to words in phrases as well as words in normal search input. Content search can only stem words for the language it has been optimized for. The following languages support stemming in Content Search:

- English
- French
- German
- Italian
- Spanish
- Dutch
- Swedish
- Portuguese
- Russian
- Polish

The following languages do not support stemming in Content Search:

- Japanese

- Traditional Chinese
- Simplified Chinese
- Korean

Content Search excludes all non-alphanumeric characters from searches and indexing.

Because Content Search creates matches based on words, it is very important that the division between words be recognized by the search system correctly. For western languages, words are tokenized based on white space or a change in character type (from alphabetical to numeric or alphabetical to special characters). Asian languages must be tokenized differently because white space is not necessarily present between words (though Content Search will recognize white space in Asian languages as signaling a break between words). Furthermore, the actual length of a word may be a single character or a combination of characters, depending on the context. Content Search tokenizes Asian languages two characters at a time, to optimize the relevance of the search results returned.

Multilingual search

Documents stored in your BusinessObjects Enterprise repository may contain text in any supported language. A report that has its language set to Japanese may contain English text for company, product, or customer names.

Languages can be combined in a single search with Content Search.

Each language has its own rules for stemming and stop words. The rules for the language that Content Search has been optimized for are applied at index time across all documents. This means that text in multilingual searches that is not in the language that content search is optimized for will not have stop words or stemming rules applied when the search is executed; all search input text will be compared literally to indexed text. If a stop word is included in a multilingual search in a language that Content Search is not optimized for, results that may be related to your search but do not include the stop word are not included. If your search input includes words (in a language other than the language for which Content Search is optimized) that are not written in the normalized form, matches to other forms of the word are not recognized and do not create results.

Content Search and instances

Content Search will return report instances that match the search input. The top five matching instances, ranked by relevance, are listed beneath the parent object. There is a link to a listing of all matched instances of that object.

Facets and labels

Facets and labels or automatic categorization is the way Content Search enables users to look at only a specific subset of their search results. The subsets of results that they can choose to view are created based on characteristics of the search results, which may be shared between several result objects. Each subset is called a facet. Characteristics which could be used as facets to classify the objects include object type, parameter values used in the objects, or data inside the report content.

Each facet is then broken down into specific values for that facet, called labels. The objects are associated with the labels to which it corresponds for that facet. For example, if the result objects are being classified by the data source facet, the labels underneath it would include the names of universes used by the objects.

This makes it easier to narrow your focus when looking at a list of search results, even if you don't know what other search words you might need to add. You are presented with the different facets and labels to choose from and can decide which to look at, even if you did not know that you might have those options when you started the search.

Prompts and Parameters

Prompts and parameters, which are supported by Crystal reports, Web Intelligence documents, and Desktop Intelligence documents, are indexed. In instances, only the current parameter values are indexed. In parent objects, potential values are also indexed. Potential values include:

- The default value of the parameter.
- The values in a static pick list for the parameter.

- The LOV associated with the prompt for Web Intelligence and Desktop Intelligence documents.

When a report with prompts or parameters appears as a search result without any saved data, data will need to be collected from the database if the user decides to view it. This will require the prompt or parameter values to be filled in.

If default parameter or prompt settings have been designated for the object, those settings will be respected. If the object is set to prompt the user for a new value, and the search text matches any of the potential parameter values that have been indexed, Content Search will fill in the parameter with that matching value.

Reports with view time security

Crystal reports have view time security if any of the following conditions are met by the report:

- The report is based on a business view.
- The report uses a processing extension.
- The report is based on a universe.

If a Crystal report with view time security appears as a search result, users will not be able to see data they do not have the necessarily rights to access. Due to performance considerations, Content Search does not index the saved data in reports with view time security. Even if a user has the rights to view the saved data, they cannot base searches on that data because it was not indexed; instead, searches must be based on static text or metadata in the report for it to appear as a search result.

For Crystal reports based on universes, you can remove the restriction of view time security for specific reports.

To remove view time security on a Crystal report.

1. Go to the **Folders** management area of the CMC.
2. Navigate to the Crystal report for which you want to disable view time security.
3. Select the report and click **Manage** and **Default Settings**.
4. Click **Viewing Server Group**.

5. Under **Universe-related settings**, select the **Generate Static Instances for Scheduling** option.
6. Click **Save & Close**.

Suggested queries

Rather than looking for a specific object, a user may be trying to find answers to a specific question when using Content Search. These answers may or may not be answered in reports that exist in your BusinessObjects Enterprise repository, and they may also be answered by creating a new object.

By analyzing the structure of universes and of existing reports in your BusinessObjects Enterprise repository and comparing this information to the search terms the user inputs, Content Search can suggest new Web Intelligence queries that may help users find the answers to their questions.

To create potential reports, Content Search matches the words in the name of a universe, measure, filter value, or other related metadata.

Content Search looks for matches in the following information about universes or existing Web Intelligence or Desktop Intelligence documents:

- Measures in universes that match words in the search input.

When a measure matches one of the search terms, that measure will be used in the resulting Web intelligence document.

- Dimension names in universes that match words in the search input.

When a dimension name matches one of the search terms, the resulting Web Intelligence document breaks down the information on this dimension.

- Query filters may be used to focus the data show in the document. These query filters are generated by analyzing the search input.
 - If the name of a universe condition matches one of the search terms, the condition is used as the filter.
 - If there are field values in existing Web Intelligence or Desktop Intelligence documents whose names match search terms, a filter will be created from the dimension from the historical report with the matched value, using "equal to" as the condition operator.

If Content Search has made enough matches that the resulting document will contain two result fields and one filter, the query is considered to be “ready to run”. In this case, the user can click to view the completed report.

If there are an insufficient number of matches between universes and the document, users are able to edit the query before running it.

Content Search will suggest multiple documents if several universes match the search input, or if the same word appears in two different matches, such as in the name of a dimension and as a filter value.

The new document suggestion presented to the user takes the user's rights into account. Only when the user has all the necessarily rights to complete the operation will the system present the suggested document. In particular, the users need the following rights:

- The right to create Web Intelligence documents.
- View and Data Access rights to the universe and dimensions involved.

Limited number of search results

Users may unintentionally conduct searches that are very broad and return a very large number of matches. This can put a large load on your system, so the maximum number of hits returned by a search is set to 1000 by default.

Excluding documents from Content Search

There are cases where you may choose to exclude documents from search indexing for performance considerations. For example, you may not want extremely large Crystal reports to be searchable out of consideration for report application server resources; similarly, you may not want publications with hundreds of personalized reports to be indexed. For this reason, a corporate category named “Exclude From Search” is created by the installer.

The Exclude From Search category signals the system that documents belonging to the category must be excluded from indexing. By associating particular documents to this category, the administrator can prevent them from being accessed via Content Search. It is important to note that if a document has been indexed before it is put into the category, the document may still be searchable. To ensure documents in the Exclude From Search

category are not searchable, you should rebuild the index by using the **Reset index when the indexing program object next runs** option on the Content Search application page.

By default, the Administrator account has full control access to the Exclude From Search category, and other groups and users have no access. The security rights which determine who can add a document to a category apply. In particular, users need the following rights in order to add a document to the Exclude from Search category:

- View and Edit rights on the category
- Edit right on the document

Related Topics

- [About categories](#)
- [How rights work in BusinessObjects Enterprise](#)

Servers and architecture

There are four main components of Content Search -- the application, the indexing program, the search services, and the search index.

The application controls Content Search. You can access its settings from the "Applications" management area of the CMC and determine who can administer Content Search, indicate your search language, and reset the index if you need to.

The indexing program is a program object that is installed with Content Search. It is placed in a top-level folder in the BusinessObjects Enterprise repository called "Search Program". When the indexing program runs, it crawls through all the objects in the repository and indexes all the "tokens"—essentially the ideological unit of the search language—so that users can search for them. You must run the indexing program once before you enable Content Search so that all tokens are correctly indexed, and then set up a recurring scheduling job to run the indexing program regularly.

The search services extract contents from documents to create the index and run any queries against the index. They are hosted by the Adaptive Processing Server. If your deployment is expected to experience a large number of simultaneous search requests, you can set up several search services to balance the load between them.

The search index is stored in a designated location on the file system (not in the CMS repository or the File Repository Server) and contains all tokens in all searchable documents that are indexed. When the indexing program runs, it creates and updates the index. When a user searches with Content Search, it is this index that is checked for their search terms, so it is important to run the indexing program often enough that the search index is kept up to date with the content of objects in your repository.

There are also two categories created and used by Content Search. You can assign objects to the “Excluded from Content Search” category if you do not want them to be indexed. If, while the indexing program is running, it is unable to index an object, it assigns that object to the “Content Indexing Failures” category. These system attempts to index objects in this category the next time the indexing program object runs, regardless of its modification time. You can then choose to exclude these objects from indexing by adding them to the “Excluded from Content Search” category, or edit them to make them indexable.

Deploying the Content Search service

Planning your Content Search deployment

Estimating user load

The amount of computing resources required to run Content Search depends largely on user load.

The user load of your system is the estimated number of simultaneous user search requests. This number is the basis of all other sizing calculations. The number of users on your system affects this number, but how and when your user base uses Content Search is also extremely important. The following example illustrates how the user load may be estimated:

Example: Estimating user load

Number of user accounts in the system: 5000

Estimated number of user logged on to the system at one time: 500 (10% of the total population)

Estimated number of simultaneous search requests: 50 (10% of logged on users)

Processors

The number of processors that your Content Search deployment requires depends on many factors, including the estimated user load, search performance expectation, complexity of data, and hardware constraints. The following rule of thumb may be used as an initial estimate:

1 CPU per 25 simultaneous requests

Memory

The total physical memory required can be estimated by the maximum heap size setting of each search service, multiplied by the number of search services in the deployment. The default maximum heap size setting of a search service is 512MB. The recommended number of search services is one for every 25 simultaneous requests.

For example, for a system with an estimated user load of 50 simultaneous requests, the estimated physical memory required to run Content Search, with search services set to the default heap size setting, would be:

$(50 / 25) * 512\text{MB} = 1\text{GB}$

Disk space

Disk space is required to store the index of your BusinessObjects Enterprise content. The size of the index will depend on both the number of objects in the system, as well as the size and data complexity in the objects.

As a rule of thumb, the disk space allocated to store the index should be of the same order of magnitude as the total file size in the File Repository (including both the Input and Output repository servers).

Installation and Upgrade

Content Search is part of BusinessObjects Enterprise and is installed along with the rest of a system installation or upgrade. All of the same installation options and configurations supported by BusinessObjects Enterprise are supported by Content Search.

The following installation sub-options, which you can choose to install when you install BusinessObjects Enterprise, are required to use Content Search:

- Adaptive Processing Server

Configuration

Managing Content Search application settings

The Content Search application is accessed through the "Applications" management area of the CMC. From the "Properties" dialog box for the Content Search application, you can configure the following settings:

- Reset the index
- Set the search language
- Set the index location
- Set the maximum number of objects indexed concurrently

To determine when your BusinessObjects Enterprise repository is indexed, you must set the scheduling options for the indexing program object.

From the rights page of the Content Search application page, you can set the rights for administrators to change Content Search properties.

These settings will not be transferred over from one system to another during migration/importing.

Note:

When you change any of the properties of the Content Search application except **Resent index when the indexing program object next runs**, you must restart all search services in your deployment.

Related Topics

- [Reset index when the indexing program object next runs](#)
- [Setting the search language](#)
- [Setting the index location](#)
- [Set maximum number of documents indexed concurrently](#)
- [Managing the indexing program object](#)
- [Setting rights for the Content Search application](#)

Reset index when the indexing program object next runs

Use the reset index property when you want to rebuild your index. You may want to do this if the index is corrupted, or after you have relocated the index to a different disk. You must also reset the index when you change the search language for which the index is optimized.

When you select the reset index checkbox, the index will be reset the next time the indexing program object runs. It is important to note that:

- The index will not be reset if the indexing process is already running. If the indexing process is running, go the history page of the indexing program to stop the job, then reset the index and reinitialize the indexing program job.
- The Content Search service will index all content in the CMS repository. The time that this takes depends on the quantity of content; therefore, it is important that you allow enough time for the process to complete before attempting to search for content and before you run the indexing program job again.

Once the index is reset, the system deselects this option automatically.

Tip:

To reset your index, go to the **Applications** management area of the CMC. Select the Content Search application, click **Manage** and then **Properties**. Select the **Resent index when the indexing program object next runs** and click **Save & Close**.

Setting the search language

Setting the search language will apply stemming and stop-word rules according to the grammar and lexicon of the target language. For example, if you set English as the search language, the system will be optimized to return results for English searches. A user who types “a walk” in their InfoView Content Search box will see results for “walking” and “walked”.

After you change your search language, you must restart your search service. You must also reset your index, so that it contains appropriate stemming and stop word information about the content of all of your objects.

Note:

Stemming does not affect searches in Chinese, Japanese, and Korean because stemming is not applicable for these languages.

To set the search language

1. Go to the "Applications" management area of the CMC.
2. Select the Content Search application.
3. Click **Manage** and **Properties**.
4. Choose the new search language from the **Search language** list.
5. Select **Reset index when indexing program next runs**.

After you reset the search language, you must restart the search services.

Setting the index location

You can change the location of the index in the **Set index location** field. For example, if the disk where the index is currently located is nearing capacity, you will want to move the index to another disk and indicate its location here.

Note:

If your deployment has multiple search services (hosted in the Adaptive Processing Servers), the index location must be a valid file path to each of these server processes.

To move the index

1. Stop the Adaptive Processing Server.

2. On the indexing program object's history page, pause the pending indexing job.
3. Copy the index directory from the current disk to a new disk.
4. Go to the "Applications" management area of the CMC
5. Select the **Content Search** application.
6. Click **Manage > Properties**.
7. Type the new index location in the **Index Location** field.
8. When the scheduled time of the indexing job arrives, the job proceeds to update the index in the new location.
9. Start the Search service.

Set maximum number of documents indexed concurrently

When setting the maximum number of documents to be indexed concurrently, consider the following:

- A higher concurrence will result in faster indexing.
- A higher concurrence requires more computing resources, and therefore will compete with other services on the system.

Your setting will depend on your unique environment, and the relative value you place on speed versus resource allocation. The default number of documents indexed concurrently is 1.

Tip:

To set the maximum number of objects to be indexed concurrently, go to the **Applications** management area of the CMC. Select the Content Search application, click **Manage** and then **Properties**. Type the appropriate number in the **Maximum number of objects indexed concurrently** field and click **Save & Close**.

To set the maximum number of objects indexed concurrently

1. Select the Content Search application.
2. Click **Manage** and **Properties**.
3. Enter the number of objects to index concurrently in the **Maximum number of objects indexed concurrently** field.
4. Click **Save & Close**.

After you set the maximum number of objects to index concurrently, you must restart the search services.

To restart the search services

You must restart the search servers after you change any of the properties settings of the Content Search application, except **Reset index when the indexing program object next runs**.

1. Go to the "Servers" management area of the CMC.
2. Select the Adaptive Processing Server.
3. Click **Actions** and **Restart server**.

Setting rights for the Content Search application

You set rights to the Content Search application object from the rights tab of the Content Search application page.

Only users who have edit rights to this application can modify the setting of the search service.

Related Topics

- [How rights work in BusinessObjects Enterprise](#)
- [Overview](#)

Disabling and removing Content Search

The availability of the Content Search service in InfoView to each user is determined by whether the user has the right to Do a Content Search on the InfoView application.

If there is a need to selectively grant or deny the use of Content Search to a user or group, you can grant or deny Do a Content Search rights on the InfoView application. When users who do not have the Do a Content Search right to the InfoView application log on to InfoView, the **Search Content** option is disabled.

Related Topics

- [To modify security for a principal on an object](#)

Maximum group instances indexed

Maximum Group Instances Indexed

When a Crystal Report document with saved data is indexed, the group instances (that is, the nodes as shown on the group tree) in the document are extracted. Such information will be consumed by the Search Server to generate search result facets and labels, as seen on the left hand side Navigation pane of the search results.

For large and complex reports, the group tree can be very large. The memory consumption by the search service during indexing of a Crystal Report document is directly related to the number of group instances it needs to process; the more group instances will result in bigger memory consumption. By default, the system extracts at most 10000 group instances from a report.

The search services should be restarted after the properties file is changed.

To change the maximum number of group instances indexed

1. Open the file `\installation directory\common\4.0\java\lib\plugins\cr\indexer.properties` where *installation directory* is the directory in which BusinessObjects Enterprise is installed.
2. Find the following line of code:
`indexer.CrystalReport.maximumNumberOfGroups=10000`
3. Replace “1000” with the maximum number of group instances to index Crystal reports.
4. Save the file

Note:

Make this change on each server machine where the Adaptive Processing Server that hosts the Search services is running.

After you have changed the maximum number of group instances to index, you must restart the search services.

JVM Heap Size

The default heap size setting the search service is 512MB. This should be a good starting point for most deployments. However, if the search service is configured to index multiple documents concurrently, a bigger maximum heap size may be needed.

With a maximum heap size of 512 MB, the maximum number of objects indexed concurrently should be not be set to a number greater than 4. With a higher concurrence, the maximum heap size should be adjusted proportionally. For example, a configuration of 8 concurrently indexed documents should be accompanied with a maximum heap size of 1GB.

To set the JVM heap size

1. Go to the "Servers" management area of the CMC
2. Select the Adaptive Processing Server that hosts the search service.
3. Click **Manage** and **Properties**.
4. In the **Command Line Properties** field, add the following additional options:

"-Xms x "

Replace x with the initial size, in bytes, of the memory allocation pool.

"-Xmx y "

Replace y with the maximum size, in bytes, of the memory allocation pool.

Note:

Both values must be a multiple of 1024 and must be greater than 1MB. To specify either number in kilobytes, add a letter k or K after the number. To specify the either number in megabytes, add a letter m or M.

5. Click **Save & Close**.

Note:

You must restart the Adaptive Processing Server for the changes to take effect.

6. Select the Adaptive Processing Server that hosts the search service.
7. Click **Actions** and **Restart Server**.

Understanding and managing the indexing process

Preparing for the initial indexing

The first time the indexing process runs it will attempt to index all documents in the BusinessObjects Enterprise repository. The time it takes will vary, depending on the number of objects in the system and their size and complexity.

Before you run the indexing job for the first time, there are best practices that you should follow. Disable Content Search, so that users do not get incomplete results set because they have searched an incomplete index. Choose and configure the search language you wish Content Search to be optimized for, because how the BusinessObjects Enterprise repository is indexed varies depending on which language is set as the search language.

Disabling Content Search in preparation for the initial indexing

Before you index your BusinessObjects Enterprise repository for the first time, you should disable Content Search. This will prevent your users from searching an incomplete index, which would return incomplete results and potentially create confusion. When the initial indexing job is completed, you can enable Content Search again.

To disable Content Search, you must make sure that your users do not have the right to Use Content Search on the InfoView application in the CMC. You should ensure that the Everyone group has no access to Content Search.

Related Topics

- [Preparing for the initial indexing](#)

- *To assign principals to an access control list for an object*

Choosing and configuring the search language

The search language option on the Content Search application manage page in CMC determines which language the system uses for language sensitive searching capability. When Content Search indexes the system, it looks for stop words and words which need to be stemmed based on the language it is set to use. Thus, changing the search language requires you to rebuild the entire index. So that you have to rebuild the entire index as infrequently as possible, this setting should be configured properly before the initial indexing. After you change this setting, you must restart the search service.

Related Topics

- *Setting the search language*

Creating the initial index

After you have finished preparing for the initial indexing, you should start the initial indexing job by scheduling the index program to run. You should choose a time when your system is not under a high user load to maintain high performance for your users.

After you have created the index, you should also create a recurring schedule on which to run the indexing program object to keep your search index up to date and to ensure that your users get the most up to date search results.

Related Topics

- *Preparing for the initial indexing*
- *Scheduling the indexing program object*

Managing the indexing program object

The indexing program object indexes the documents in the repository in order to make them searchable. It is scheduled to run regularly to maintain

the index of the objects in BusinessObjects Enterprise. The indexing program object is managed like any other program object in the BusinessObjects Enterprise environment.

When the indexing program runs, it crawls through content and creates the index used by the search service. The servers that must be running and enabled for the indexing program object to run successfully:

- The report servers
- The CMS

Each indexing job indexes 500 objects. When that batch of 500 objects is finished, Content Search creates a new batch for the next batch of 500 objects, and continues creating new batches when the previous batch is completed until all objects are indexed.

Each time the indexing program object runs, it only indexes documents that have been changed since the last time the indexing program ran. When Content Search cannot index an object, it assigns the object to the "Content Indexing Failure" public category.

All objects in this category are re-indexed the next time the indexing program runs, regardless of how recently they were changed.

Depending on the number, size, and complexity of indexable objects in your deployment of BusinessObjects Enterprise, the indexing program object may take some time to run. It may also use a considerable amount of shared system resources, which can impact users. It is important that the recurrence schedule for the indexing program object does not occur more frequently than necessary to keep the index as up to date as is practically useful. You should also consider the peak use hours of your system and schedule the indexing program object to run when it will have a minimum impact on users.

This section provides information on:

- Scheduling the indexing program object
- Setting rights for the indexing program object

Indexing is triggered by scheduling a program object specifically installed for the search service.

The indexing program object is not visible by non-administrators, to avoid confusing users. Administrators can grant the appropriate rights to other users if they need to view or edit the indexing program object.

Related Topics

- [Scheduling](#)
- [How rights work in BusinessObjects Enterprise](#)
- [Program object management](#)

Scheduling the indexing program object

You must schedule the indexing program object so that your BusinessObjects Enterprise repository is indexed regularly. If you do not index your repository often enough, Content Search will not return accurate results because it searches the most recent index of your repository. However, indexing can take time and use significant system resources, so it should not be done too frequently. You should index on a recurring schedule or calendar so that it will run with a frequency that reflects how quickly your repository changes. Ensure that you schedule the indexing program to run when your system is not under a high server load.

After the initial indexing, the indexing program object will only index objects that have changed since the last time it was run. This is called “incremental indexing” and cuts down on the server resources needed to run subsequent indexing jobs. Only objects with a last updated time that is more recent than the last indexing time are indexed when the indexing program object runs. If necessary, you can set Content Search to completely rebuild the index, but you must do so manually.

Tip:

To schedule your indexing program object, navigate to it, select it, click **Manage** and then click **Schedule** or **History** to access the program object’s “Scheduling” and “History” dialog boxes. From the “History” dialog box, you can:

- Request a new schedule
- Suspend or stop indexing
- Find the success/failure status of completed indexing jobs
- See the run time of indexing
- Read error messages from the output of the program job

You can schedule two indexing jobs to run at overlapping times. The index server should be able to facilitate such requests without resulting in any corruption of the index.

Related Topics

- [Reset index when the indexing program object next runs](#)
- [Scheduling](#)
- [Program object management](#)

Setting rights for the indexing program object

The indexing program object is installed in a new top-level folder called “Search Program.” By default, the installer grants explicit full control access to this folder to the administrator, and explicitly denies access for the “Everyone” group.

For more information about setting rights and inheritance see [How rights work in BusinessObjects Enterprise](#). For more information about program objects, see [Program object management](#).

Terminating the indexing process

If you want to stop indexing when the indexing program job has already started, you should do so by disabling the search services, allowing the current batch of 500 objects to finish indexing, and then delete the job for the next batch of 500 objects.

Each indexing program job handles no more than 500 objects at a time. If there are more documents in the system to be indexed, it spawns another job to finish indexing.

Disabling the search services will not interrupt the batch of 500 objects being indexed by the program job at the time. However, it prevents subsequent jobs from indexing the rest of the content.

If the job running when you disabled the search services spawns another job to index the rest of the repository, the new job runs one minute after the first job completes. You can either delete this pending job or wait until the job starts and fails because the search services are disabled.

This method is preferable to stopping the Adaptive Processing Server abruptly while the indexing program job is running, which would terminate the running job before it finished the current batch of 500 objects. This may cause the indexing program job that stopped to leave behind a lock file. If this happens, you must clean up the system.

Do not delete a running instance of the indexing program job in the CMC to terminate the indexing process. This will not terminate background processing of the job.

Related Topics

- [To clean up after unplanned system downtime](#)

To terminate an indexing process

1. Go to the "Servers" management area of the CMC.
2. Select the Adaptive Processing Server.
3. Click **Actions** and **Disable Server** to disable all search services.
4. Navigate to the indexing program object and select it.
5. Click **Actions** and **History**.
6. Wait until the current indexing program job has completed and click **Refresh**.
7. Select the pending indexing program job.
8. Click **Delete**.
9. Go to the "Servers" management area of the CMC and select the Adaptive Processing Server.
10. Click **Actions** and **Enable Server** to re-enable the search services.

Troubleshooting

To troubleshoot an indexing failure

1. Go to the "Servers" management area of the CMC and ensure that the Adaptive Processing Server is running and enabled.
If it is not running or enabled, start and enable the Adaptive Processing Server, and retry indexing if necessary.

2. Navigate to the indexing program select it.
3. Click **Actions** and **History**.
4. Click **status** to observe the error message for the failed indexing program job.

When individual objects fail to index, their names appear in the error message.

5. Go to the "Servers" management area of the CMC and ensure that the reporting servers are running and enabled.
If the reporting servers are not enabled or running, start/enable them and retry the indexing if necessary.
6. Go to the "Content Indexing Failure" category and identify objects that have failed.
7. Try to view each failed object.

A document that cannot be viewed cannot be indexed.

If any of the failed objects are Web Intelligence documents, try to edit the document. A Web Intelligence document that cannot be edited cannot be indexed.

8. Move all objects that cannot be viewed, and Web Intelligence documents that cannot be edited, to the "Exclude from Content Search" category so that the indexing program will not attempt to index them again and retry indexing.
9. Examine the search service log files in `\installation directory\Logging\`, where *installation directory* is the path to the directory in which you installed BusinessObjects Enterprise.
The search service log files are named by the convention `SearchServer_nnnnnnnnnn.log`. You can obtain detailed error messages can be obtained from the log file.

To clean up after unplanned system downtime

In the event of an abrupt termination of the search service, such as a sudden power outage, some locks may be left on the index, which prevents subsequent indexing from succeeding. You can unlock the instance by following this procedure.

1. Go to the "Servers" management area of the CMC.

2. Select the Adaptive Processing Server.
3. Click **Actions** and **Stop Server** to stop all search services.
4. Navigate to the indexing program object and select it.
5. Click **Actions** and **History**.
6. Ensure that all jobs that were running have terminated.
7. Delete all files in `\installation directory\Data\search\lockDir\`, and all files and subdirectories in `\installation directory \Data\search\working\` , where *installation directory* is the path to the directory in which BusinessObjects Enterprise is installed.
8. Go to the "Servers" management area of the CMC and select the Adaptive Processing Server .
9. Click **Actions** and **Enable Server** to re-enable the search services.
10. If the lock has prevented one of your indexing jobs from running, reschedule the indexing program object to ensure that the search index is up to date.



Rights Appendix

29



chapter

About the rights appendix

This rights appendix lists and describes most rights that can be set on different objects in the BusinessObjects Enterprise 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 and the BusinessObjects Enterprise rights model, see the *Setting Rights* chapter in the *SAP BusinessObjects Enterprise Administrator's Guide*.

General rights

The rights in this section apply to multiple object types.

Note:

- 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. For more information about owner rights, see [Owner rights](#).
- The following rights only apply 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 BusinessObjects Enterprise 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.
"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 Choosing between Modify the rights users have to objects options .
"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.

Right	Description
"Copy objects to another folder"	<p>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.</p> <p>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.</p>
"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"	<p>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.</p> <p>To schedule an object for other users or groups, you also require the following rights:</p> <ul style="list-style-type: none"> • This right on the user or group. • The "Schedule the document to run" right on the object.

Right	Description
"Schedule to destinations"	<p>Lets you do the following:</p> <ul style="list-style-type: none">• Schedule objects to destinations other than the default Enterprise location.• Modify the default destinations specified for scheduling. <p>To schedule the object to destinations, you also require the following rights:</p> <ul style="list-style-type: none">• 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).
"View document instances"	<p>Lets you view object instances. This right is a basic right that is required for all tasks that you perform on object instances.</p>

Right	Description
"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.

Rights for specific object types

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).

Related Topics

- [Type-specific rights](#)

Categories

The rights in this section are general rights that have a specific meaning in the context of public and personal categories.

Note:

Objects in categories do not inherit rights that are set on the categories.

Right	Description
"Add objects to the folder"	Lets you create new categories within categories. This right is not needed to add objects to a category.
"Edit objects"	<p>Lets you do the following:</p> <ul style="list-style-type: none">• Modify category properties.• Move the category into another category as a sub-category.• Add objects to the category.• Remove objects from the category. <p>To move a category into another category as a sub-category, you also require the following rights:</p> <ul style="list-style-type: none">• 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.

Notes

Notes allow users to comment on other objects using the Discussions application. Notes are linked together in discussion threads; these discussion threads are considered child objects of the objects that they discuss. You can set rights at the object level or folder level to control the use of discussion threads.

The rights in this section apply to notes only.

Right	Description
Allow discussion threads	<p>This right lets you do the following:</p> <ul style="list-style-type: none">• Start and reply to discussion threads.• View notes on a discussion thread.• Modify or delete notes that you posted.

Crystal reports

The rights in this section apply to Crystal reports only.

Note:

These rights only apply when Crystal reports are in the BusinessObjects Enterprise 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"	<p>Lets you export report data to any format when you view the report online in the Crystal Reports viewer.</p> <p>To export report data in RPT format, you also require the "Download files associated with the object" right.</p>
"Download the files associated with the object"	<p>This right lets you do the following:</p> <ul style="list-style-type: none">• Export the report in RPT format.• Open the report in Crystal Reports Designer.• Schedule the report in RPT format to external destinations.

Desktop Intelligence documents

Desktop Intelligence document rights can exist at the document level and at the application level. Rights applied at the document level are enforced when you view or edit the document in InfoView, the HTML Viewer, and the CMC. Rights applied at the application level are enforced when you open documents in Desktop Intelligence. This means that users may have more rights than intended if they view or edit Desktop Intelligence documents outside of the BusinessObjects Enterprise environment. To prevent this, you can deny the following rights:

- The "Retrieve documents" right at the application level.
- The "Download files associated with the object" right at the document level.
- The "Export the report's data" right at the document level.

Right	Description
"Refresh the report's data"	Lets you refresh document data.
"Refresh List of Values"	Lets you refresh the lists of values available for prompts. To refresh the lists of values, you also require the "Use List of Values" right.
"Use Lists of Values"	Lets you use and refresh lists of values in the document.
"View SQL"	Lets you view the SQL used for queries.
"Export the report's data"	Lets you export or download document data. To download document data, you also require the "Download files associated with the object" right.
"Download files associated with the object"	Lets you download the document from the CMS. To download a document, you also require the following rights: <ul style="list-style-type: none"> • The "Export the report's data" right on the document. • The "Retrieve documents" right at the application level.

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.
"View SQL"	Lets you view the SQL for queries.
"Export the report's data"	Lets you export document data to Excel, PDF, and CSV formats. If you do not have this right, you require the "Save as CSV", "Save as Excel", or "Save as PDF" right; these rights let you export documents in the specified format only.
"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.

Right	Description
"Save as CSV"	Lets you export documents as CSV files only. If you have the "Export the report's data" right on a document already, you do not require this right.
"Save as Excel"	Lets you export documents as Excel files only. If you have the "Export the report's data" right on a document already, you do not require this right.
"Save as PDF"	Lets you export documents as PDF files only. If you have the "Export the report's data" right on a document already, you do not require this right.

Users and groups

You can set rights on users and groups as you would on other objects in the BusinessObjects Enterprise environment. The rights in this section are type-specific rights that apply to user and group objects only or general rights that have a specific meaning in the context of users and groups.

Note:

- Users and subgroups can inherit rights from group membership.
- The creator of a user account is considered the owner of the account. However, after the user account is created, the user that the account is intended for is also considered an owner.

Right	Description
"Edit objects"	<p>Lets you do the following:</p> <ul style="list-style-type: none">• Edit properties for the user or group.• Manage group membership. <p>To add a user or group to another group, you require this right on the user or group and on the destination group.</p>
"Change user password"	<p>Lets you do the following:</p> <ul style="list-style-type: none">• 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. <p>Note:</p> <ul style="list-style-type: none">• This right does not affect the following user password settings:<ul style="list-style-type: none">• "Password never expires"• "User must change password at next logon"• "User cannot change password"• This right does not apply to data source credentials for Business Objects Universes.
"Subscribe to publications"	<p>Lets you add the user to publications as a recipient.</p>
"Schedule on behalf of other users"	<p>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.</p>

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.

Related Topics

- [Choosing between Modify the rights users have to objects options](#)

Dashboards

The rights in this section are general rights that control specific user actions in the context of dashboards.

Right	Description
"Add objects to this folder"	<p>Lets you add menus to the dashboard. However, this right does not let you add analytics or other objects to the dashboard.</p> <p>To add a menu to the dashboard, you also require the "Access to Application Builder" right.</p>
"Edit objects"	<p>This right lets you do the following:</p> <ul style="list-style-type: none">• Edit dashboard properties and content.• Edit dashboard menus.• Delete a dashboard. <p>To edit dashboard content, you also require the "Customize Module Page" right.</p>

Analytic rights and dashboards

Analytics are graphical components that measure changes in the values of specific metrics over a certain period of time. Analytics can be used to build dashboards.

How analytics are added to the repository affects their security settings. If you add analytics to the repository as autonomous objects, you can set general rights on the analytics themselves; these rights are enforced when the analytics are used in dashboards. If you save an analytic in a dashboard and then add the dashboard to the repository, the analytic inherits the rights that are set on the dashboard.

Universes

The rights in this section 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 when you import universes from the CMS in the Designer 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.
"Edit objects"	<p>This right lets you do the following:</p> <ul style="list-style-type: none"> Edit the universe in the CMC or in Designer. Lock or unlock the universe. <p>To unlock a universe, you also require the "Unlock Universe" right.</p>
"New List of Values"	<p>This right lets you do the following:</p> <ul style="list-style-type: none"> Associate new lists of values with objects. Edit existing lists of values. <p>Note: This right does not prevent you from creating cascading lists of values.</p>
"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.

Right	Description
"Unlock Universe"	Lets you do the following: <ul style="list-style-type: none">• 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 Designer 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.

Universe objects

When you design a universe in the Designer application, you can designate certain objects within the universe as Public, Controlled, Restricted, Confidential, or Private. Once you export the universe to the CMC, access to universe objects can be granted based on the object-level security settings you made in the Designer application. For example, you can grant the Everyone group access to all objects designated as Public.

Each object level security setting grants more access to objects than the previous one. Public is the most restrictive setting and only lets principals access objects designated as Public, Controlled is less restrictive and lets principals access objects designated as Public and Controlled, and so on. Private is the least restrictive setting and grants principals access to all objects within the universe.

To set object-level security, you require the **Modify the rights users have to objects** right on the universe.

Note:

- Object-level security settings override any security settings that the universe inherits.
- More restrictive object-level security settings override the less restrictive ones.

Connections

The rights in this section are type-specific rights that apply to universe connections only or general rights that have a specific meaning in the context of universe connections.

Right	Description
"View objects"	Lets you view the connection.
"Data Access"	Lets you retrieve content from the database specified for the connection. The content can consist of data or database schemas in Designer. If this right is denied, you cannot retrieve data from the database in Designer.
"Use connection for Stored Procedures"	<p>Lets you use the stored procedures in the database specified for the universe connection.</p> <p>Note: The connection must be a secure connection saved in the CMS.</p>

Applications

CMC

The rights in this section apply to the CMC only.

Right	Description
"Log on to the CMC and view this object in the CMC"	Lets you log on to the CMC.
"Allow access to Instance Manager"	Lets you access the Instance Manager.
"Allow access to Relationship Query"	Lets you run relationship queries in the CMC.
"Allow access to Security Query"	Lets you run security queries in the CMC.

InfoView

The rights in this section apply to InfoView only.

Right	Description
"Change user's preferences"	Lets you change your InfoView preferences such as your default viewers and displayed fields.
"Organize"	Lets you do the following: <ul style="list-style-type: none">• Move and copy objects.• Add objects to your Favorites folder.• Create shortcuts to objects.
"Search for simple text"	Lets you run simple searches.
"Do an advanced search"	Lets you run advanced searches.
"Do a content search"	Lets you run content searches.

Right	Description
"Filter object listing by object type"	Lets you filter objects in the Details panel according to object type.
"View the favorites folder"	Lets you view and access your Favorites folder.
"View the Inbox"	Lets you view your InfoView inbox.
"Create categories"	Lets you create personal or public categories. To do this, you also require the "Add objects to the folder" right on the category in which you want to create a subcategory.
"Assign categories"	<p>Lets you assign objects to categories. To do this, you also require the following rights:</p> <ul style="list-style-type: none"> • The "View objects" right on the category and the object. • The "Add objects to the folder" right on the category. • The "Edit objects" right on the destination category.

Right	Description
"Send documents"	Lets you send objects to email, inbox, FTP, or local file destinations.
"Create dashboards"	Lets you create dashboards in InfoView.
"Create folders"	Lets you create personal or public folders. To do this, you also require the "Add objects to the folder" right on the folder in which you want to create the new folder.

Desktop Intelligence

You can use Desktop Intelligence in three modes: online, offline, and standalone. The rights and credentials that you require for Desktop Intelligence depend on the mode that you use:

- If you use Desktop Intelligence in online mode, you need valid logon credentials that are checked against your user account in the CMS. The rights that your user account has determine which actions you can perform in the application.
- If you use Desktop Intelligence in offline mode, you need valid logon credentials that are checked against cached credentials.
- If you use Desktop Intelligence in standalone mode, no logon credentials are required and no rights are applied. However, to allow all users to open a saved Desktop Intelligence document in Desktop Intelligence in standalone mode, the user who saved the document must have the "Save for all users" right on the document.

The rights in this section apply to the Desktop Intelligence application only.

Right	Description
"Create Desktop Intelligence Documents"	Lets you create new documents.
"Create Templates"	Lets you save documents as templates.
"Use Templates"	Lets you do the following: <ul style="list-style-type: none"> • Create documents with templates. • Apply templates to existing documents.
"Save Desktop Intelligence Documents"	Lets you save documents to local disk. Note: If the "Save for all users" right is not also granted, only the document owner can open the document.
"Save documents for all users"	Lets you save documents on local disk so that all users can view them with Desktop Intelligence in offline or standalone mode. To do this, you also require the "Save Desktop Intelligence Documents" right.
"Desktop Intelligence Document Interaction"	Lets you rename, copy, insert, and delete report tabs in documents.
"Desktop Intelligence Report Interaction"	Lets you edit report tab content.
"Refresh Desktop Intelligence Document"	Lets you refresh document data. To do this, you also require the "Refresh the report's data" right on the document.
"Print Documents"	Lets you print documents.
"Copy to Clipboard"	Lets you cut or copy document content.

Right	Description
"Euro Converter"	Lets you convert currency figures in documents to and from Euros.
"Edit Euro Converter Rate"	Lets you modify the exchange rates that are used by the Euro Converter.
"Drill Through"	Lets you drill further when you view document data.
"Edit Scope of Analysis"	Lets you set the scope of analysis.
"Work in Drill Mode"	Lets you drill up or down in documents.
"Work in Slice-and-Dice Mode"	Lets you use the Slice and Dice Panel.
"Edit VBA Code"	Lets you edit VBA macros in documents.
"Run VBA Code"	Lets you run VBA code.
"Install Add-Ins"	Lets you install and uninstall VBA add-ins.
"Manage All Corporate Categories"	Lets you create, edit, and delete corporate categories in Desktop Intelligence.
"Manage My Corporate Categories"	Lets you create, edit, and delete personal categories in Desktop Intelligence.
"Refresh Document List and Categories"	Lets you refresh category lists and category contents.
"Send Documents to Repository"	Lets you export documents to public or personal folders in the CMS. To do this, you also require the "Add objects to this folder" right on the destination folder.

Right	Description
"Send Documents to Mail"	Lets you send documents as emails in Desktop Intelligence.
"Send Documents to Inbox"	Lets you send documents to InfoView inboxes.
"Retrieve Documents"	Lets you import documents from personal or public folders in the CMS into Desktop Intelligence.
"Create And Edit Connections"	Lets you create new data source connections or edit existing connections.
"Data Provider Manipulation"	Lets you modify queries or the universes that are queried.
"Edit Free-hand SQL"	Lets you edit queries that use free-hand SQL scripts as data providers. To do this, you also require the "Use Free-hand SQL" right.
"Use Free-hand SQL"	<p>Lets you use free-hand SQL to create queries.</p> <p>Note: This right does not affect the ability to refresh a document that uses free-hand SQL queries.</p>
"Edit Personal Data Files"	Lets you edit parameters for personal data providers in Desktop Intelligence.
"Use Personal Data Files"	<p>Lets you create documents using Excel, dBASE, or ASCII text files as data providers.</p> <p>Note: This right does affect the ability to refresh a document that uses personal data providers.</p>
"Edit Stored Procedures"	Lets you edit parameters for stored procedures.

Right	Description
"Use Stored Procedures"	Lets you create documents using Stored Procedures as data providers.
"Always Regenerate SQL"	<p>Lets you force SQL queries to refresh when the document data refreshes.</p> <p>Note: This right can affect overall document processing performance. If there is no specific need for this right, it is recommended that you set it to Denied or Not Specified.</p>
"Edit Query SQL "	<p>Lets you edit the SQL in queries. To do this, you also require the following rights:</p> <ul style="list-style-type: none"> • The "Edit Queries" right. • The "View SQL" right.
"Use other SQL requests than Select"	<p>Lets you use SQL clauses other than SELECT. To do this, you also require the following rights:</p> <ul style="list-style-type: none"> • The "Edit Queries" right. • The "View SQL" right. • The "Edit Query SQL" right.
"View SQL "	Lets you see the SQL that queries generate.
"Edit Queries"	Lets you edit queries.
"Use Queries"	Lets you create new queries that are based on universes.
"Edit Lists of Values"	Lets you edit lists of values in universes.

Right	Description
"Use List of Values"	Lets you use lists of values in universes.
"Refresh List of Values"	Lets you refresh lists of values in universes.
"Use User Objects"	Lets you create, edit, and delete user objects.

Web Intelligence

The rights in this section apply to Web Intelligence and Web Intelligence Rich Client only and can affect viewers and query panels in these applications.

Right	Description
"Edit SQL"	Lets you modify the SQL used in queries. To do this, you also require the following rights: <ul style="list-style-type: none"> • The "View SQL" right on the document. • The "Edit Query" right on the document.
"View SQL"	Lets you view the SQL used in queries.
"Merge dimensions for synchronization"	Lets you merge dimensions or objects from different data providers.
"Enable interactive HTML viewing"	Lets you display Web Intelligence documents in the interactive viewer.
"Enable Query - HTML"	Lets you edit and create Web Intelligence documents using HTML queries.

Right	Description
"Enable HTML Report Panel"	Lets you edit and create Web Intelligence documents using the HTML Report Panel.
"Enable Java Report Panel"	Lets you edit and create Web Intelligence documents using the Java Report Panel.
"Extend scope of analysis"	Lets you retrieve data and drill up or down in documents beyond the initial scope of analysis.
"Enable drill mode"	Lets you drill up or down in documents.
"Create document"	Lets you create new Web Intelligence documents.
"Data Tracking: Enable for users"	Lets you use the Track Data Changes feature.
"Data Tracking: Enable format display changes by users"	Lets you modify the format that the Track Data Changes feature uses.
"Interactive: General - Enable right click menu"	In the interactive viewer, lets you right-click on an object and use the options in the context menu.
"Interactive: Left pane - Enable document summary"	Lets you display the document summary in the left pane of the interactive viewer.
"Interactive: Left pane - Enable data summary"	Lets you display the data summary in the left pane of the interactive viewer.
"Interactive: Left pane - Enable document structure and filters"	Lets you display the document structure and filters in the left pane of the interactive viewer.

Right	Description
"Interactive: Left pane - Enable available objects, tables and charts"	Lets you display the list of available objects, tables, and charts in the left pane of the interactive viewer.
"Interactive: Formatting - Enable toolbar and menus"	Lets you use the formatting features in the interactive viewer.
"Interactive: Reporting - Create and edit report filter"	Lets you create and edit filters in the interactive viewer.
"Interactive: Reporting - Create and edit sort"	Lets you create and edit sorts in the interactive viewer.
"Interactive: Reporting - Create and edit break"	Lets you create and edit breaks in the interactive viewer.
"Interactive: Reporting - Create and edit predefined calculation"	Lets you create and edit predefined calculations in the interactive viewer.
"Interactive: Reporting - Create and edit alerters"	Lets you create and edit alerters in the interactive viewer.
"Interactive: Reporting - Insert report, table, chart and cell"	Lets you insert reports, tables, charts, and cells in the interactive viewer.
"Interactive: General - Ability to hide / show toolbars"	Lets you show or hide the Formatting, Report, and Formula toolbars in the interactive viewer.
"Interactive: General - Edit 'My Preferences'"	Lets you edit your preferences for the interactive viewer.
"Enable formula and variable creation"	Lets you use the formula editor feature.

Right	Description
"Web Intelligence Rich Client: Create a document"	Lets you create new Web Intelligence documents in Web Intelligence Rich Client.
"Web Intelligence Rich Client: Enable a client to use it"	Lets you use Web Intelligence Rich Client.
"Web Intelligence Rich Client: Export a document"	Lets you export documents to the BusinessObjects Enterprise repository in Web Intelligence Rich Client.
"Web Intelligence Rich Client: Import a document"	Lets you import documents from the BusinessObjects Enterprise repository into Web Intelligence Rich Client.
"Web Intelligence Rich Client: Install from InfoView"	Lets you install Web Intelligence Rich Client from InfoView.
"Web Intelligence Rich Client: Print a document"	Lets you print documents in Web Intelligence Rich Client.
"Web Intelligence Rich Client: Remove document security"	Lets you remove document security in Web Intelligence Rich Client so that any principal can view or modify the document in Web Intelligence Rich Client.
"Web Intelligence Rich Client: Save a document for all users"	Lets you save documents so that all users can open and view them in Web Intelligence Rich Client.

Right	Description
"Web Intelligence Rich Client: Save a document locally on the file system"	Lets you save documents on local disk in Web Intelligence Rich Client.
"Web Intelligence Rich Client: Send by mail"	Lets you send documents as emails in Web Intelligence Rich Client.
"Web Intelligence Rich Client: Allow local data providers"	Lets you create new documents using personal data providers in Web Intelligence Rich Client.

Performance Management

The rights in this section apply to Performance Management only. Performance Management rights can be divided conceptually into the following categories:

- Analysis

These rights affect Set Analysis, particularly the Individual Profiler module.

- App Foundation

These rights let users access different menus and sections in Dashboard Builder, Set Analysis, Process Analysis, and Predictive Analysis.

- Configuration

These rights let users perform certain tasks in Dashboard Builder, Set Analysis, Process Analysis, and Predictive Analysis.

- Rules

These rights affect rules and the actions that are triggered by rules.

- Services Bar

These rights enable icons and links in the toolbar.

Depending on the task that you want to perform, you may require different rights from different categories.

To access any component of Performance Management, you require at least these rights:

- The **Access to Performance Management** right on the Performance Management application.
- The **Use Performance Management** right on the Performance Management application.
- The **Log on to InfoView and view this object in the CMC** right on the InfoView application.

Analysis rights for Performance Management

The rights in this section affect the Individual Profiler module in Performance Management. To access the Individual Profiler module, you require at least these rights:

- The "Schedule Sets Refresh" right.
- The "Access to Sets Menu" right.

Right	Description
"Individual Profiler - Access to Portrait"	In Set Analysis, lets you access the Portrait portion of Individual Profiler.
"Individual Profiler - Access to Membership"	In Set Analysis, lets you access and create Membership analytics that let you view the selected set for a specified period. To manage Membership, you also require these rights: <ul style="list-style-type: none">• The "Schedule Sets Refresh" right.• The "Access to Sets Menu" right.
"Individual Profiler - Access to Metrics"	In Set Analysis, lets you access metrics lists that are associated with sets.

App Foundation rights for Performance Management

The rights in this section affect different menus and sections in Dashboard Builder, Set Analysis, Process Analysis, and Predictive Analysis.

Right	Description
"Access to Metric Definition"	<p>In Dashboard Builder, lets you define metrics and metric trees. To work with metrics, you also require these rights:</p> <ul style="list-style-type: none"> • The "Edit metric" right. • The "Define Sliced Metrics - Ability to select a dimension when creating a metric" right. • The "Refresh or Purge Metrics" right.
"Access to Lists Menu"	<p>In Set Analysis, lets you define lists that are used to export data or meta data.</p>
"Access to Rules Menu"	<p>In Dashboard Builder, lets you access the "Rules" page. To perform additional tasks, you also require these rights:</p> <ul style="list-style-type: none"> • The "View Public Rules" right to view public rules. • The "Edit Public Rules" right to create public rules. • The "Edit Private Rules" right to create private rules.
"Access to Schedule Menu"	<p>In Dashboard Builder, lets you schedule metrics, sets, control charts, analytics, and models. To do this, you also require the "Edit Schedule - Access to the scheduler menu" right.</p> <p>Note: Before you schedule objects in Dashboard Builder, the Scheduler and required server credentials must be configured properly.</p>

Right	Description
"Analytics Catalog"	In Dashboard Builder, lets you drag and drop analytic templates from the catalog and edit them in corporate or personal dashboards while you are in customization mode. You can only use analytics that correspond to areas that you can access.
"Access to Sets Menu"	Lets you use Set Analysis.
"Access to Control Charts"	<p>In Process Analysis, lets you access the "Control Charts" page and view control charts. Control charts are Process Analysis analytics that plot variations in process outcomes over periods of time.</p> <p>To create, modify, delete, and refresh control charts, you also require these rights:</p> <ul style="list-style-type: none">• The "Edit Control Charts" right.• The "Refresh Control Charts" right.
"Access to Population Definition"	<p>In Predictive Analysis, lets you access the "Population" page and view populations. Populations are named queries that define groups of interest.</p> <p>To create, modify, delete, and refresh populations, you also require the "Edit Populations - Controls" right.</p>

Right	Description
"Access to Derived Variables"	<p>In Predictive Analysis, lets you access the "Derived Variables" page and see derived variable definitions. Derived variables are user-defined data elements that derive from universe objects or memberships.</p> <p>To create, modify, delete, and refresh derived variables, you also require the "Edit Derived Variables - Controls the ability to create, edit, or remove derived variables" right.</p>
"Access to Model Definition"	<p>In Predictive Analysis, lets you access the "Models" page and view models. Models are configurations of the predictive calculation engine that are designed by users. Users select influencers, goals, and populations to design models.</p> <p>To create, modify, delete, and refresh models, you also require these rights:</p> <ul style="list-style-type: none"> • The "Edit Models - Controls the ability to create, edit, or remove models" right. • The "Refresh Statistics or Regenerate Model" right.
"Access to Create New Analytic Menu"	<p>In Dashboard Builder, lets you create new analytics.</p>
"Access to Analytic Services"	<p>In Dashboard Builder, lets you drag and drop analytic services and edit them in corporate or personal dashboards in customization mode. You can only use analytics that correspond to areas that you can access.</p>

Right	Description
"Access to system setup Repository and System User tabs"	Lets you use the system setup options and define the system user for application engines. To do this, you also require the "Access to System Setup" right.
"Access to system setup Universes and Dimensions tabs"	<p>Lets you do the following:</p> <ul style="list-style-type: none"> • Define universes that contain multiple metrics. • Export universes that contain multiple metrics to the repository. • Use the dimensions for sliced analysis. <p>To perform these tasks, you also require the "Access to System Setup" right.</p>
"Access to setup Time Config tab"	Lets you define the Calendar and Period properties that are used by time-based analysis. To do this, you also require the "Access to System Setup" right.
"Access to setup Parameters tab"	Lets you specify parameters for the application. To do this, you also require the "Access to System Setup" right.
"Access to setup Tools tab"	Lets you access and use the "Tools" tab. To do this, you also require the "Access to System Setup" right.
"Access to setup Control Charts tab"	Lets you create samplings, alarms, and filters that are used to create control charts. To do this, you also require the "Access to System Setup" right.

Configuration rights for Performance Management

The rights in this section let users perform certain tasks in Dashboard Builder, Set Analysis, Process Analysis, and Predictive Analysis.

Right	Description
"Customize Module Page"	In Dashboard Builder, lets you design dashboards and add analytics to them. To do this, you also require the "Edit objects" right on the dashboard.
"Schedule Sets Refresh"	In Dashboard Builder, lets you create scheduled tasks for the "Set Refresh" function.
"Edit Metric"	In Dashboard Builder, lets you create, modify, and delete metrics. To do this, you also require the "Access to Metric Definition" right.
"Define Sliced Metrics - Ability to select a dimension when creating a metric"	In Dashboard Builder, lets you select a dimension when you create metrics. To do this, you also require the "Access to Metric Definition" right.
"Edit Schedule - Access to the scheduler menu"	In Dashboard Builder, lets you modify recurrence and run parameters for metrics, sets, control charts, analytics, and models. To do this, you also require the "Access to Schedule Menu" right.
"Customize My Dashboards"	In Dashboard Builder, lets you customize "My Dashboards".
"Edit Documents - Ability to add/edit/delete a Web Intelligence document"	In Dashboard Builder, lets you access the query panel to create or edit Web Intelligence documents.

Right	Description
"Edit Control Charts"	In Process Analysis, lets you create, delete, and modify control charts. To do this, you also require the "Access to Control Charts" right.
"Refresh Control Charts"	In Process Analysis, lets you refresh and purge control charts. To do this, you also require the "Access to Control charts" right.
"Edit Populations - Controls the ability to create, edit, or remove populations"	In Predictive Analysis, lets you create, modify, and delete populations. To do this, you also require the "Access to Population Definition" right.
"Edit Derived Variables - Controls the ability to create, edit, or remove derived variables"	In Predictive Analysis, lets you create, modify, and delete derived variables that are based on universe objects. To do this, you also require the "Access to Derived Variables" right.
"Edit Models - Controls the ability to create, edit, copy, or remove models"	In Predictive Analysis, lets you create, modify, and delete models. To do this, you also require the "Access to Model Definition" right.
"Edit Data Mining Metrics - Controls the ability to create, edit, or remove data mining metrics"	In Predictive Analysis, lets you create metrics that are based on existing models.
"Edit Binning - Controls the ability to create, edit, or remove bins for predictive analysis"	In Predictive Analysis, lets you create, modify, and delete binning based on universe objects. To do this, you also require the "Access to Derived Variables" right.

Right	Description
"Refresh Statistics or Regenerate Model"	In Predictive Analysis, lets you re-fresh or regenerate existing models.
"Refresh or Purge Metrics"	Lets you purge or refresh metrics so that refreshed data is available. If you refresh the metrics on demand, you also require the "Access to Metric Definition" right; if the metrics are scheduled to refresh or purge themselves, you do not require the "Access to Metric Definition" right.
"Preview Analytics"	Lets you preview analytics that have multiple viewer options. In preview mode, the analytic appears as a static entity and cannot be refreshed.
"Send email - Controls the ability to email an analytic"	In Dashboard Builder, lets you email analytics.

Rules rights for Performance Management

The rights in this section apply to rules that you define in the Dashboard Builder.

To add actions to rules, you require these rights in addition to the right that applies to the action you want to add:

- The "Edit Public Rules" right for public rules.
- The "Edit Private Rules" right for private rules.
- The "Access to Rules Menu" right.

Tip:

You can prevent users from creating rules that allow control charts to refresh or rules that allow sets to refresh. To do this, set the "Refresh Control Charts" right or the "Schedule Set Refresh" right to Denied.

Note:

If all the rights in this section are denied to users, users can still create rules, but these rules will be useless because they do not contain any actions.

Right	Description
"Actions - Raise an Alert"	Lets you add the raise an alert action to rules.
"Actions - Send an Email"	Lets you add the send an email action to rules.
"Actions - Define a List"	Lets you add the define a list action to rules.
"Actions - Generate an Event"	Lets you add the generate an event action to rules.
"Actions - Refresh a Report"	Lets you add the refresh a report action to rules.
"Actions - Generate a URL"	Lets you add the generate a URL action to rules.
"Actions - Refresh Metrics"	Lets you add the refresh metrics action to rules.
"Actions - Launch an Application"	Lets you add the launch an application action to rules.
"Actions - Execute SQL"	Lets you add the execute SQL action to rules.
"View Public Rules"	In Dashboard Builder, lets you view all public rules. To do this, you also require the "Access to Rules Menu" right.
"Edit Public Rules"	In Dashboard Builder, lets you create, modify, and delete public rules. To do this, you also require the "Access to Rules Menu" right.

Right	Description
"Edit Private Rules"	In Dashboard Builder, lets you create, modify, and delete private or personal rules. To do this, you also require the "Access to Rules Menu" right.
"Edit Private Folders"	In Dashboard Builder, lets you create, modify, and delete private folders that are used by rules.
"Edit Public Folders"	In Dashboard Builder, lets you create, modify, and delete public folders that are used by rules.

Services Bar rights for Performance Management

The rights in this section affect icons and links in the toolbar for Performance Management.

Right	Description
"Access to Performance Management"	Lets you use Performance Management. You also require the "Use Performance Management" right.
"Options"	Lets you change Performance Management preferences in InfoView.
"Access to My Dashboards"	Lets you use "My Dashboards" to manage dashboards.
"Access to System Setup"	Lets you administer Performance Management and set parameters.

Strategy Builder

Strategy Builder is a tool related to Performance Management. The rights in this section apply to Strategy Builder only and can affect goals management in Performance Manager or specific features in Strategy Builder.

Right	Description
"Create, Modify, or Delete Goals"	Lets you add, edit, or remove goals in Performance Manager.
"View Goals"	Lets you see goals in analytics that contain goals.
"Access to Goal Management"	Lets you view goals on the "Goals Management" page in Performance Manager.
"Publish Goals"	Lets you publish goals in Performance Manager.
"Access to Strategy Builder"	Lets you access the Strategy Builder tool in Performance Manager.
"Create, Modify, or Delete Roles"	Lets you administer the roles that are used to publish goals or metrics to specific audiences in Strategy Builder.
"Create, Modify, or Delete Strategies"	Lets you create strategies that link roles and publish goals and metrics in Strategy Builder.

Designer

The rights in this section apply to the Designer application only.

Right	Description
"Check Universe Integrity"	Lets you check universe integrity.
"Refresh Structure Window"	Lets you refresh the structure window.
"Use Table Browser"	Lets you view database data using the table browser.
"Apply Universe Constraints"	Lets you apply predefined universe constraints to users of an imported universe.
"Link Universe"	Lets you link two universes and share components.
"Create, Modify or Delete Connections"	Lets you create, modify, and delete universe connections that are stored in the CMS or stored as personal or shared connections.

BI Widgets

The rights in this section apply to the BI Widgets application only.

Right	Description
"Use Explorer"	Lets you use the BI Widgets Explorer.
"Use Alert Inbox"	Lets you use the Alerts Inbox.
"Use Search"	Lets you use the search functionality.
"Use BI Widgets"	Lets you use BI Widgets.
"Use Open Widgets from Disk"	Lets you use the Open from Disk functionality in BI Widgets.

Polestar

The rights in this section apply to Polestar only.

Right	Description
"Log on to Polestar and view this object in the CMC"	Lets you log on to Polestar. This right is required for you to perform other tasks with Polestar.
"Explore Information Spaces"	Lets you explore an Information Space. To perform this task, you must also have the "Log on to Polestar and view this object in the CMC" right.
"Explore Information Spaces: Export to Bookmark/Email"	Lets you bookmark and email bookmarks. To perform this task, you must also have the following rights: <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Explore Information Spaces"
"Explore Information Spaces: Export to CSV"	Lets you export the results of an exploration to a CSV. To perform this task, you must also have the following rights: <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Explore Information Spaces"
"Explore Information Spaces: Export to Image"	Lets you export the results of an exploration as an image. To perform this task, you must also have the following rights: <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Explore Information Spaces"

Right	Description
"Explore Information Spaces: Export to Web Intelligence"	<p>Lets you export the results of an exploration as a query.</p> <p>To perform this task, you must also have the following rights:</p> <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Explore Information Spaces"
"Manage Information Spaces "	<p>Lets you access the Manage Spaces menu and perform the associated tasks.</p> <p>To perform this task, you must also have the "Log on to Polestar and view this object in the CMC" right.</p>
"Manage Information Spaces: Create a new Space"	<p>Lets you create a new Information Space.</p> <p>To perform this task, you must also have the following rights:</p> <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Manage Information Spaces "

Right	Description
"Manage Information Spaces: Modify a Space"	<p>Lets you modify or delete an Information Space.</p> <p>To perform this task, you must also have the following rights:</p> <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Manage Information Spaces "
"Manage Information Spaces: Schedule indexing"	<p>Lets you schedule indexing for Information Space data.</p> <p>To perform this task, you must also have the following rights:</p> <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Manage Information Spaces "
"Manage Information Spaces: Launch indexing"	<p>Lets you run indexing for Information Space data.</p> <p>To perform this task, you must also have the following rights:</p> <ul style="list-style-type: none"> • "Log on to Polestar and view this object in the CMC" • "Manage Information Spaces "



Server Properties Appendix



30 chapter

About the server properties appendix

This server properties appendix lists and describes properties that can be set for each BusinessObjects Enterprise server. For more information about server properties, see the *Improving Performance* chapter in the *SAP BusinessObjects Enterprise Administrator's Guide*.

Common Server Settings

The server settings described in this section apply to all server types.

Request Port Settings

Property	Description	Default Value
Request Port	<p>Specifies the port from which the server receives requests from other servers. You may want the server to listen for requests on a specific port. For example, in an environment with firewalls, you may want to force the server to only listen to requests on ports that are open on the firewall.</p> <p>Note: If Auto assign is selected, the server binds to a dynamically allocated port.</p>	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. To bind the server to a specific port, set Auto Assign to FALSE and specify a valid Request Port .	The default value is TRUE.

Server Intelligence Agent Settings

Property	Description	Default Value
Automatically start this server when the Server Intelligence Agent starts	<p>Specifies whether the server is automatically started when the Server Intelligence Agent (SIA) starts or restarts.</p> <p>If this value is set to FALSE and the SIA starts or restarts, the server remains stopped.</p>	The default value is TRUE.

Host Identifiers

Property	Description	Default Value
Auto assign	Specifies whether the server binds to a specific network interface, or whether the network interface is automatically assigned. On multihomed machines, you can specify a particular network interface to bind to by setting this value to FALSE and providing a hostname or IP address.	The default value is TRUE.
Hostname	The hostname of the network interface that the server binds to.	A valid host-name.
IP Address	The IP address of the network interface that the server binds to. Both IPv4 and IPv6 protocols are supported.	A valid IPv4 or IPv6 address.

Configuration Template Settings

Property	Description	Default Value
Use Configuration Template	Specifies whether to use a configuration template for all services of the same type as the current service. For more information on working with configuration templates, see Working with configuration templates .	The default value is FALSE.
Restore System Defaults	Specifies whether to restore the original default settings for the particular server type.	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. For more information on working with configuration templates, see Working with configuration templates .	The default value is FALSE.

Core Server Settings

The Core services category includes the following servers:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Destination Job Server
- Event Server

- Input File Repository Server
- Output File Repository Server
- Program Job Server
- Publication Job Server
- Web Application Container Server

Adaptive Job Server Settings

Property	Description	Default Value
Maximum Concurrent Jobs	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You adjust the maximum number of jobs to suit your reporting environment.</p> <p>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.</p> <p>Note: You must restart the server for changes to take effect.</p>	The default value is 5.
Temporary Directory	<p>Specifies the directory where temporary files are created on when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	%Default DataDir%

Adaptive Processing Server Settings

Property	Description	Default Value
Service Startup Timeout (seconds)	<p>Specifies the amount of time, in seconds, that the server will wait for services to start.</p> <p>If a service fails to start within the time specified, there are two possible reasons:</p> <ul style="list-style-type: none"> • 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. <p>To find the reason, check the server log file. If the service could not start within the time specified, consider increasing this value.</p>	The default value is 300 seconds.
Maximum size of the thread pool	<p>Specifies the maximum number of working threads allowed in the thread pool.</p> <p>If you want the maximum size of the thread pool to be dynamically calculated based on the number of CPUs available in your system, specify "0".</p>	The default value is 50.

Property	Description	Default Value
Log level	<p>Specifies the minimum severity of warning that you want to be recorded, and determines how much information is recorded in the server log file.</p> <p>The Adaptive Processing Server uses industry-standard log4j logging provided by Apache Software Foundation (http://logging.apache.org/log4j).</p> <p>Five log threshold levels are provided by log4j, in decreasing level of severity:</p> <ul style="list-style-type: none"> • FATAL • ERROR • WARN • INFO • DEBUG <p>In a production environment, we recommend setting the log level to ERROR so that only ERROR and FATAL messages are generated and non-essential messages are suppressed.</p>	<p>The default logging level is set to AUTO. The AUTO logging level is the equivalent of ERROR.</p>

Central Management Server Settings

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Table 30-7: Central Management Service Settings

Property	Description	Default Value
Name Server Port	Specifies the port on which the CMS listens to name service requests.	The default value is 6400.

Property	Description	Default Value
System Database Connections Requested	Specifies the number of CMS database connections CMS attempts to establish.	The default value is 14.
Disable Auto Reconnect to System and Auditing Databases	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.	The default value is FALSE.

Table 30-8: Single Sign-on Service

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.

Destination Job Server Settings

Property	Description	Default Value
Maximum Concurrent Jobs	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You adjust the maximum number of jobs to suit your reporting environment.</p> <p>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.</p> <p>Note: You must restart the server for changes to take effect.</p>	The default value is 5.
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	%Default DataDir%

Event Server Settings

Property	Description	Default Value
Cleanup Interval (minutes)	Specifies how often cleanup utility runs, in minutes.	The default value is 20 minutes.
Event Poll Interval (minutes)	Specifies how often the server polls for a file that triggers an event, in minutes.	The default value is 10 minutes.

Input File Repository Server Settings

Property	Description	Default Value
Maximum Re-tries for File Access	Specifies the number of times the server tries to access a file.	The default value is 1.
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.	The default value is 10 minutes.
Temporary Directory	Specifies the directory where temporary files are created when necessary. Note: You may encounter performance issues if this directory does not have adequate disk space.	%DefaultInputFRSDir/temp%
File Store Directory	Specifies the directory where repository objects are stored.	%DefaultInputFRSDir/%

Output File Repository Server Settings

Property	Description	Default Value
Maximum Re-tries for File Access	Specifies the number of times the server tries to access a file.	The default value is 1.

Property	Description	Default Value
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.	The default value is 10 minutes.
Temporary Directory	Specifies the directory where temporary files are created when necessary. Note: You may encounter performance issues if this directory does not have adequate disk space.	%DefaultOutput FRSDir/temp%
File Store Directory	Specifies the directory where repository objects are stored.	%DefaultOutput FRSDir/%

Program Job Server Settings

Property	Description	Default Value
Maximum Concurrent Jobs	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You adjust the maximum number of jobs to suit your reporting environment.</p> <p>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.</p> <p>Note: You must restart the server for changes to take effect.</p>	The default value is 5.
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	%Default DataDir%

Publication Job Server Settings

Property	Description	Default Value
Maximum Concurrent Jobs	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You adjust the maximum number of jobs to suit your reporting environment.</p> <p>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.</p> <p>Note: You must restart the server for changes to take effect.</p>	The default value is 5.
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	%Default DataDir%

Web Application Container Server Settings

Table 30-15: General Properties

Property	Description	Range of Values
Log level	<p>Specifies the minimum severity of warning that you want to be logged. The DEBUG level logs the most amount of activity, and the FATAL logs the least amount; only critical messages are logged.</p> <p>It is not recommended to set the log level to DEBUG or INFO in a production environment, because this may affect server performance.</p> <p>Changing the log level does not require that you restart the WACS.</p>	<p>The levels that are available, in increasing level of severity are:</p> <ul style="list-style-type: none"> • AUTO • DEBUG • INFO • WARN • ERROR • FATAL <p>By default, the AUTO level is set to ERROR.</p>
Service Startup Timeout (seconds)	<p>Specifies the amount of time, in seconds, that the server will wait for its hosted services to start before it times out. If the timeout passes, the WACS will not provide CMC services. On a slower machine, you can consider specifying a longer value.</p> <p>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).</p>	<p>The default value is 300 seconds.</p>

Table 30-16: Concurrency Settings (Per Connector)

Property	Description	Default Value
Maximum Concurrent Requests	Specifies the number of concurrent HTTP or HTTPS requests that each connector (HTTP, HTTP through Proxy, or HTTPS) can process simultaneously.	The default value is 150. The valid range is 1 to 1000.

Table 30-17: Active Directory Configuration Settings

Property	Description	Default Value
Krb5.ini File Location	Specifies the full name of a <code>krb5.ini</code> file that stores Kerberos configuration properties.	The full name of the <code>krb5.ini</code> file.
bscLogin.conf File Location	Specifies the full name of a <code>bscLogin.conf</code> file.	The full name of the <code>bscLogin.conf</code> file.

Table 30-18: HTTP Configuration Properties

Property	Description	Default Value
Bind to All IP Addresses	Specifies 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.	The default value is TRUE.
Bind to Hostname or IP Address	Specifies the network interface (IP address or hostname) on which HTTP service is provided. You can only specify a value if you uncheck Bind to All IP Addresses .	The default value is localhost.

Property	Description	Default Value
HTTP Port	Specifies the port on which HTTP service is provided.	The default value is 6405. The valid range is 1 to 65535.

Table 30-19: Configuration of HTTP through Proxy

Property	Description	Default Value
Enable HTTP through Proxy	Specifies whether to enable the HTTP through Proxy connector on the WACS. This is typically checked in deployments with a reverse proxy.	The default value is FALSE.
Bind to All IP Addresses	Specifies whether to bind the HTTP through proxy port to all network interfaces or not.	The default value is TRUE.
Bind to Host-name 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 .	The default value is localhost
HTTP Port	Specifies 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 .	The default value is 6406. The valid range is 1 to 65535.
Proxy Host-name	Specifies 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 .	By default, this value is empty.

Property	Description	Default Value
Proxy Port	Specifies the port of your forward or reverse proxy server. You can only specify a value if you check Enable HTTP through Proxy .	By default, this value is empty. The valid range is 1 to 65535.

Table 30-20: HTTPS Configuration

Property	Description	Default Value
Enable HTTPS	Specifies whether to enable HTTPS/SSL communication.	The default value is False.
Bind to Host-name 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 .	The default value is localhost.
HTTPS Port	Specifies the port on which HTTPS service is provided. You can only specify a value if you check Enable HTTPS .	The default value is 443. The valid range is 1 to 65535.
Proxy Host-name	Specifies 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 .	By default, this value is empty.
Proxy Port	Specifies the port of your forward or reverse proxy server. You can only specify a value if you check Enable HTTPS .	By default, this value is empty. The valid range is 1 to 65535.
Protocol	Specifies the encryption protocol to use. You can only specify a value if you check Enable HTTPS .	The default value is TLS.

Property	Description	Default Value
Certificate Store Type	Specifies 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 .	The default value is PKCS12.
Certificate Store File Location	Specifies the full name to the certificate file. You can only specify a value if you check Enable HTTPS .	By default, this value is empty.
Private Key Access Password	Specifies the password for your private keys. 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 .	By default, this value is empty.
Certificate Alias	Specifies 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 .	By default, this value is empty.
Enable Client Authentication	Specifies whether to 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 .	The default value is FALSE.

Property	Description	Default Value
Certificate Trust List File Location	Specifies the full name of the certificate trust list file. You can only specify a value if you check Enable HTTPS and Enable Client Authentication .	By default, this value is empty.
Certificate Trust List Private Key Access Password	Specifies 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 .	By default, this value is empty.

Crystal Reports Server Settings

The Crystal Reports service category includes the following servers:

- Crystal Reports Cache Server
- Crystal Reports Job Server
- Crystal Reports Processing Server
- List of Values Job Server
- Report Application Server

Crystal Reports Job Server Settings

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Property	Description	Range of Values
Maximum Concurrent Jobs	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You adjust the maximum number of jobs to suit your reporting environment.</p> <p>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.</p>	The default value is 5.
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	%Default DataDir%

Crystal Reports Cache Server Settings

Any properties that apply to both Crystal Reports Cache Servers and Crystal Reports Processing Servers should be set to the same value. For example, if you set the **Viewer Refresh Always Yields Current Data** setting to TRUE on the Cache Server, you should set the same property to TRUE on the Processing Server.

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Property	Description	Range of Values
Viewer Refresh Always Yields Current Data	<p>Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database.</p> <p>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.</p>	The default value is TRUE.
Share Report Data Between Clients	<p>Specifies whether report data is shared between different clients.</p> <p>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.</p>	The default value is TRUE.
Idle Connection Timeout (minutes)	<p>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.</p>	The default value is 20 minutes.

Property	Description	Range of Values
Oldest On-Demand Data Given to Clients (seconds)	<p>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.</p> <p>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.</p>	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

Crystal Reports Processing Server

Any properties that apply to both Crystal Reports Cache Servers and Crystal Reports Processing Servers should be set to the same value. For example, if you set the **Viewer Refresh Always Yields Current Data** setting to TRUE on the Cache Server, you should set the same property to TRUE on the Processing Server.

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Table 30-23: Crystal Reports Processing Service

Property	Description	Range of Values
Idle Job Time-out (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 60 minutes.
Database Records Read When Previewing or Refreshing (0 for unlimited):	Specifies the maximum number of database records to read when the report is being previewed or refreshed. It allows you to limit 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 containing queries 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.
Maximum Lifetime Jobs Per Child	Specifies the maximum number of jobs that each child process can manage per lifetime.	The default value is 1000.

Property	Description	Range of Values
Viewer Refresh Always Yields Current Data	<p>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.</p> <p>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.</p>	The default value is TRUE.
Share Report Data Between Clients	<p>Specifies whether report data is shared between different clients. Specifies whether report data is shared between different clients.</p> <p>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.</p>	The default value is TRUE.
Idle Connection Timeout (minutes)	<p>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.</p>	The default value is 20 minutes.

Property	Description	Range of Values
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)	<p>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.</p> <p>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.</p>	The default value is 0.

Property	Description	Range of Values
Maximum Number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessary wasted by idle child processes.	The default value is 1 child.
Temporary Directory	Specifies the directory where temporary files are created when necessary. Note: You may encounter performance issues if this directory does not have adequate disk space.	%Default DataDir%/Crystal ReportsProcessingServer/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.

Table 30-24: Single Sign-On Service

Property	Description	Range of Values
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

List of Values Job Server

Note:

When you modify any of these settings, you must restart the server for the changes to take effect.

Property	Description	Range of Values
Maximum Concurrent Jobs	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You adjust the maximum number of jobs to suit your reporting environment.</p> <p>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.</p>	The default value is 5.
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	%Default DataDir%

Report Application Server Settings

Note:

When you modify any of these settings, you must restart the server for the changes to take effect.

Table 30-26: Crystal Reports Viewing and Modification Service

Property	Description	Range of Values
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 <code>ReportClientDocument</code> object is not closed explicitly, the server will be waiting unnecessarily for an idle job to close).	The default value is 30 minutes.

Property	Description	Range of Values
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 settings 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.
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.

Table 30-27: Single Sign-On Service

Property	Description	Range of Values
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Xcelsius Server Settings

The Xcelsius service category includes the following servers:

- Xcelsius Cache Server
- Xcelsius Processing Server

Xcelsius Cache Server Settings

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Property	Description	Range of Values
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Xcelsius 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.
Maximum Cache Size (KB)	Specifies the amount of hard disk space (in KB) that is used to cache queries. A large cache size may be necessary if the server needs to handle large numbers of queries, or queries that are especially complex.	The default value is 256000 KB.

Property	Description	Range of Values
Cache Files Directory	Specifies the location of the cache file directory.	%DefaultDataDir%/XcelsiusCacheServer/temp

Xcelsius Processing Server

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Table 30-29: Xcelsius Processing Service

Property	Description	Range of Values
Idle Job Timeout (minutes)	Specifies the length of time, in minutes, that the Xcelsius Processing Server waits between requests for a given job.	The default value is 60 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.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Xcelsius 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.

Property	Description	Range of Values
Maximum Concurrent Jobs (0 for automatic)	Specifies the maximum number of independent jobs allowed to run concurrently on the Xcelsius 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.
Maximum Number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessary wasted by idle child processes.	The default value is 1 child.
Temporary Directory	Specifies the directory where temporary files are created when necessary. Note: You may encounter performance issues if this directory does not have adequate disk space.	%DefaultDataDir%/XcelsiusProcessingServerServer/temp

Table 30-30: Single Sign-On Service

Property	Description	Range of Values
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Web Intelligence Server Settings

Web Intelligence Processing Server properties

The Web Intelligence Processing Server properties are grouped into the following services:

- Single Sign-On
- Web Intelligence Life Cycle Management
- Memory Management
- Web Intelligence Process Server Instance Recycling
- Tuning Dataflow and Sizing
- Cache Life Cycle Management
- Web Intelligence Caching
- Universe Caching
- List of Values Caching

Threshold settings are described in separate tables.

Single Sign-On Settings

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.

Web Intelligence Life Cycle Management Settings

Property	Description	Default Value
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.	The default value is 300 seconds. The valid range is 100-10000 seconds.

Property	Description	Default Value
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 cause requests to be queued while the server waits for idle requests to be closed.	The default value is 20 minutes.
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.	The default value is 120 seconds.
Maximum Document 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 the default value is 5, then the user can use up to 5 active sessions at once.	The default value is 5. The valid range is 1-20.
Allow Document Map Maximum Size Errors	Specifies whether the <i>Maximum Connections</i> property is restricted. If this property is enabled, then the value set for the <i>Maximum Connections</i> property is recognized by the server; otherwise the property is disregarded.	The default value is TRUE.

Property	Description	Default Value
Maximum Connections	<p>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.</p> <p>Note: The <i>Allow Document Map Maximum Size Errors</i> property must be enabled for this property to be recognized by the server.</p>	<p>The default value is 50 sessions. The valid range is 5 to 65535.</p>

Memory Management Settings

Property	Description	Default Value
Enable Memory Analysis	<p>Specifies whether memory analysis is enabled. If this property is enabled then the following properties will be active and recognized by the server:</p> <ul style="list-style-type: none"> • <i>Memory Maximum Threshold</i> • <i>Memory Upper Threshold</i> • <i>Memory Lower Threshold</i> <p>When the server's process memory is above the <i>Memory Upper Threshold</i>, the only operation that is allowed is saving documents. When the process memory is above the <i>Memory Maximum Threshold</i>, all operations stop and fail.</p>	<p>The default value is TRUE.</p>

Property	Description	Default Value
Memory Maximum Threshold (MB)	Specifies the maximum threshold for memory consumption. For more information on what happens when the server reaches this threshold, see Web Intelligence Server Memory Threshold Settings .	The default value is 1800MB. The valid range is 1000 to 2000MB.
Memory Upper Threshold (MB)	Specifies the upper threshold for memory consumption. For more information on what happens when the server reaches this threshold, see Web Intelligence Server Memory Threshold Settings .	The default value is 1500MB.
Memory Lower Threshold (MB)	Specifies the lower threshold for memory consumption. For more information on what happens when the server reaches this threshold, see Web Intelligence Server Memory Threshold Settings .	The default value is 1000MB.

Web Intelligence Processing Server Instance Recycling Settings

Property	Description	Default Value
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.	The default value is 50 documents.

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.	The default value is 1200 seconds.

Tuning Dataflow and Sizing Settings

Property	Description	Default Value
Binary Stream Maximum Size (MB)	Specifies the maximum size, in MB, of a binary stream sent to the Web Intelligence client. Note: If the Binary Stream Maximum Size property is exceeded, then the Web Intelligence document will not be created and the client will receive an error message.	The default value is 50 MB. The valid range is 1 to 65535 MB.
Maximum Character Stream Size (MB)	Specifies the maximum character stream size sent to the Web Intelligence client. Note: If the Maximum Character Stream Size property is exceeded, then the Web Intelligence document will not be created and the client will receive an error message.	The default value is 5 MB. The valid range is 1 to 65535 MB.
Maximum List of Values Size (entries)	Specifies the maximum number of entries (or values) for each List of Values.	The default value is 50000 entries per List of Values.

Property	Description	Default Value
List of Values Batch Size (entries)	Specifies the maximum number of entries (or values) for each List of Values batch.	The default value is 1000 entries per batch.
Maximum Custom Sort Size (entries)	Specifies the maximum number of entries in the custom sort.	The default value is 100 entries per custom sort.

Cache Life Cycle Management Settings

Property	Description	Default Value
Document Cache Clean-up Interval (seconds)	Specifies the time interval, in seconds, that the document cache is scanned and is checked against the <i>Maximum Document Cache Size</i> , <i>Maximum Document Cache Reduction Space</i> , and <i>Maximum Document in Cache</i> settings.	The default value is 120 seconds.
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.	The default value is 4370 minutes.
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 <i>Maximum Document Cache Reduction Space</i> property.	The default value is 1000000 KB.
Maximum Document Cache Reduction Space	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.	The default value is 70%.

Property	Description	Default Value
Maximum Document in Cache	<p>The maximum number of Web Intelligence documents that can be stored in the cache. There is never more than this many documents in the cache; the total size of the cache is never greater than the value specified with the Maximum Document Cache Reduction Space (MB) setting.</p> <p>Note: To improve system performance, set this value to 0 when <i>Enable Real-Time Cache</i> is selected, but you should enter a value when <i>Enable Real-Time Cache</i> is deselected.</p>	The default value is 0. The valid range is 0 to 65535 documents.

Web Intelligence Caching Settings

Property	Description	Default Value
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.	The default value is 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.	The default value is TRUE.

Property	Description	Default Value
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.	The default value is FALSE.
Output Cache Directory	Specifies the location of the cache.	The default value is empty.
Images Directory	Specifies the location of the images directory.	The default value is empty.

Universe Caching Settings

Property	Description	Default Value
Universe Cache Maximum Size (Universes)	Specifies the number of universes to be cached on the Web Intelligence Processing Server.	The default value is 20 universes.

List of Values Caching Settings

Property	Description	Default Value
Enable List of Values Cache	Specifies whether caching is enabled for List of Values on the Web Intelligence Processing Server.	The default value is TRUE.

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 Maximum Threshold

If the *Memory Maximum Threshold* limit is reached, all current operations abort.

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 prevent new connections and any other memory-consuming threads from starting. Only the option to **Save** Web Intelligence documents will be allowed. Users that request an action requiring memory allocation 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 delete read-only documents.
- If not enough memory was freed during system cleanup then the server will begin to close documents that are in "View" 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: $\text{Memory Upper Threshold} - (20\% * (\text{Memory Upper Threshold}))$. For example, if the Memory Upper Threshold property is set to 1500MB then the safe level would be:

$$1500\text{MB} - .20 * 1500\text{MB} = 1200\text{MB}$$

- If not enough memory was released while closing documents in "View" mode, then the server will begin to close all remaining open documents including those that are in "Edit" 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 1500MB then the safe level would be:

$$1500\text{MB} - .20 \times 1500\text{MB} = 1200\text{MB}$$

Memory Lower Threshold

If the *Memory Lower Threshold* is reached, the server will swap out inactive documents onto the hard disk, allocating additional memory for documents which are active.

Desktop Intelligence Server Settings

The Desktop Intelligence service category includes the following servers:

- Connection Server
- Desktop Intelligence Cache Server
- Desktop Intelligence Job Server
- Desktop Intelligence Processing Server

Connection Server

Property	Description	Default Value
Idle Transient Object Timeout (minutes)	Specifies how many minutes to keep unused temporary objects.	The default value is 60 minutes.
Enable HTTP Client Support	Specifies whether the Connection Server can be accessed through a CORBA server and called through an HTTP Client. This option is enabled by default to allow HTTP client communication with the Connection Server.	The default value is TRUE.

Property	Description	Default Value
Enable CORBA Client Support	Specifies whether the Connection Server can be accessed through a CORBA server and called through a CORBA client. This option is enabled by default to allow CORBA client communication with the Connection Server.	The default value is TRUE.
Enable Execution Traces	Specifies whether the Connection Server's processing activities will be tracked and monitored.	The default value is FALSE.
Idle Connection Timeout (minutes)	Specifies how many minutes before an idle connection to the Connection Server will be closed.	The default value is 60 minutes.

Desktop Intelligence Cache Server

Note:

When you modify any of these settings, you must restart the server for the changes to take effect.

Property	Description	Default Value
Viewer Refresh Always Yields Current Data	Specifies whether the report will access the database during a viewer refresh. If this property is enabled new data will be retrieved directly from the database. Otherwise a viewer refresh will serve up cached report pages.	The default value is FALSE.

Property	Description	Default Value
Cache to Keep When Document Cache is Full	<p>Specifies the percentage of the cache to keep once it has been filled. This parameter can be used to tune the cache-purge ratio. For example, if the cache is filled, but users want to keep a certain portion of it, they would use this parameter.</p> <p>Note: The server purges the cache by deleting documents with the oldest “last accessed date”.</p>	The default value is 70%. The value can be between 0% - indicating that the cache is disabled - and 100%.
Share Report Data Between Clients	Specifies whether report data is shared between different clients.	The default value is TRUE.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Cache Server waits for a request from an idle connection. Setting a value too low can cause a user's request to be closed prematurely, and setting a value that is too high can cause requests to be queued while the server waits for idle jobs to be closed.	The default value is 20 minutes.
Oldest On-Demand Data Give to Clients (seconds)	Specifies how long cached report pages are used before new data is requested from the database. This setting is respected for report instances with saved data, and for report objects that do not have on-demand subreports or parameters and that do not prompt for database logon information.	The default value is 120 seconds.

Property	Description	Default Value
Maximum Cache Size (KB)	Specifies the amount of hard disk space used to store cached pages. Once this limit has been reached, files are deleted as required to remain below this maximum value. The Desktop Intelligence Cache Server deletes the least recently used files first.	The default value is 512000KB.
Cache Files Directory	Specifies the directory where cache files will be stored.	The default install folder is / <INSTALLEDIR>/BOE12.0/Data/DesktopIntelligence-CachingServer

Desktop Intelligence Job Server

Note:

When you modify any of these server settings, you must restart the server for the changes to take effect.

Property	Description	Default Value
Maximum Concurrent Jobs	Specifies the maximum number of independent processes (child processes) allowed to run concurrently on the server. You can customize the maximum number of jobs to suit your reporting environment.	The default value is 5.

Property	Description	Default Value
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	<p>The default path is /<INSTALLED_DIR>/BOE12.0/DesktopIntelligenceCachingServer</p>

Desktop Intelligence Processing Server

Note:
When you modify any of these server settings, you must restart the server for the changes to take effect.

Property	Description	Default Value
Idle Job Timeout (minutes)	<p>Specifies the length of time, in minutes, that the Desktop Intelligence Processing Server waits for a job to complete before timing out. For example, if the property is set to 60 minutes, then the job is active for 60 minutes if no new server requests are received. However, any requests, such as normal viewing requests, continue to keep this job active. Setting a value too low can cause a user's request to be closed prematurely, and setting a value that is too high can cause system resources to be consumed for longer than necessary.</p> <p>Note:</p> <ul style="list-style-type: none"> A "job" is defined as a Desktop Intelligence report that is opened and managed within a Desktop Intelligence Processing Server. The overall timeout of the job is also influenced by the Oldest-On-Demand Data Given to Clients property. This value of this property is added to the overall timeout interval if the job has not expired. Therefore, a job is cleaned up after the sum of the following interval runs out: Oldest-On-Demand Data Given to Clients + Idle Job Timeout (minutes). 	The default value is 60 minutes.
Maximum Operations Before Re-setting a Report Job	Specifies the number of actions performed by the Desktop Intelligence Processing Server before it is re-started. It is used to ensure that servers are periodically recycled to avoid excessive memory usage and to improve system performance.	The default value is 1000.

Property	Description	Default Value
Viewer Refresh Always Yields Current Data	Specifies whether the report accesses the database during a viewer refresh. If this property is enabled then the report runs against the database. Otherwise a viewer refresh serves cached report pages.	The default value is FALSE.
Allow Running VBA	Specifies whether the Desktop Intelligence Processing server is allowed to run Visual Basic Application (VBA) scripts.	The default value is TRUE.
Share Report Data Between Clients	<p>Specifies whether the report data is shared between clients; this includes sharing both the cache and the job. A job is shared if different clients are requesting the same report and default parameters.</p> <p>Note: A “job” is defined as a Desktop Intelligence report that is opened and managed within a Desktop Intelligence Processing Server. Jobs are resource-intensive because they do not contain saved data.</p>	The default value is FALSE.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the server waits for requests from an idle connection. Setting a value too low can cause a user's request to be closed prematurely. Setting a value too high can cause system resources to be consumed for longer than necessary.	The default value is 20 minutes.

Property	Description	Default Value
Maximum Concurrent Jobs (0 for automatic)	<p>Specifies the maximum number of independent child processes allowed to run concurrently on the Desktop Intelligence Processing Server.</p> <p>Note: This property must be at least two greater than the value set for the Preloaded Report Jobs property.</p>	The default value is 10.
Oldest-On-Demand Data Given to Clients (seconds)	<p>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.</p>	The default value is 120 seconds.

Property	Description	Default Value
Preloaded Report Jobs	<p>Specifies the maximum number of preloaded jobs that are allowed by the server. Enabling this option improves server efficiency and memory allocation by recycling server processes for use by other connections without having to shut down and recreate a server instance. It also eliminates the need to create a dedicated process for each new connection.</p> <p>Note:</p> <ul style="list-style-type: none"> A “job” is defined as a Desktop Intelligence report that is opened and managed within a Desktop Intelligence Processing Server. Jobs are resource intensive because they do not contain saved data. This property must be at least two less than the value set for the Maximum Concurrent Jobs property. 	The default value is 1 job. The valid range is 0 to 10.
Temporary Directory	<p>Specifies the directory where temporary files are created when necessary.</p> <p>Note: You may encounter performance issues if this directory does not have adequate disk space.</p>	The default path is <code>/<INSTALLEDIR>/BOE 12.0/Data/DesktopIntelligenceProcessingServer</code>
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Voyager Server Settings

Multi-Dimensional Analysis Services Server

Property	Description	Default Value
Service Startup Timeout (seconds)	<p>Specifies the amount of time, in seconds, that the server will wait for services to start, before timing out if unsuccessful.</p> <p>If a service fails to start within the time specified, there are two possible reasons:</p> <ul style="list-style-type: none"> • The service failed. • The service could not start within the specified time. <p>To find the reason, check the server log file. If the service could not start within the time specified, consider modifying this value.</p>	The default value is 300 seconds.
Maximum size of the thread pool	Specifies the number of working threads.	The default value is 50 working threads. The valid range is 12 to 150.

Property	Description	Default Value
Log level	<p>Specifies the minimum severity of warning that you want to be recorded, and determines how much information is recorded in the server log file.</p> <p>The MDAS Server uses industry-standard log4j logging provided by Apache Software Foundation (http://logging.apache.org/log4j).</p> <p>Five log threshold levels are provided by log4j, in decreasing level of severity:</p> <ul style="list-style-type: none"> • FATAL • ERROR • WARN • INFO • DEBUG <p>In a production environment, we recommend setting the log level to ERROR so that only ERROR and FATAL messages are generated and non-essential messages are suppressed.</p>	<p>The default logging level is set to AUTO. The AUTO logging level is the equivalent of ERROR.</p>

Property	Description	Default Value
Maximum Client Sessions	Specifies the maximum number of Voyager sessions that can simultaneously be open on a given Multi Dimensional Analysis Server. When the number of open sessions reaches this number, any additional attempts to start Voyager 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.

Performance Management Server Settings

The Performance Management service category includes the following servers:

- Dashboard Analytics Server
- Dashboard Server
- PM Metrics Server
- PM Repository Server
- PM Rules Server
- Predictive Analysis Server
- Process Analysis Server
- Sets Profile Server
- Sets Query Server

There are no configurable server properties for these servers.



More Information



A



appendix



Information Resource	Location
SAP Analytics product information	http://www.sap.com
SAP Help Portal	<p>Navigate to http://help.sap.com/analytics and on the "Analytics" side panel click All Products, and then select the appropriate language.</p> <p>You can access the most up-to-date documentation covering all SAP Analytics products and their deployment at the SAP Help Portal. You can download PDF versions or installable HTML libraries.</p> <p>Certain guides are stored on the SAP Service Marketplace and are not available from the SAP Help Portal. These guides are listed on the Help Portal accompanied by a link to the SAP Service Marketplace. Customers with a maintenance agreement have an authorized user ID to access this site. To obtain an ID, contact your customer support representative.</p>
SAP Service Marketplace	<p>http://service.sap.com/bosap-support > Documentation</p> <ul style="list-style-type: none"> • Installation guides: https://service.sap.com/bosap-instguides • Release notes: http://service.sap.com/releasenotes <p>The SAP Service Marketplace stores certain installation guides, upgrade and migration guides, deployment guides, release notes and Supported Platforms documents. Customers with a maintenance agreement have an authorized user ID to access this site. Contact your customer support representative to obtain an ID. If you are redirected to the SAP Service Marketplace from the SAP Help Portal, use the menu in the navigation pane on the left to locate the category containing the documentation you want to access.</p>
Developer resources	<p>https://boc.sdn.sap.com/</p> <p>http://scn.sap.com/docs/DOC-27465</p>

Information Resource	Location
SAP Analytics articles and eLearning resources on the SAP Community Network	http://scn.sap.com/docs/DOC-19311 These articles were formerly known as technical papers.
Notes	https://service.sap.com/notes These notes were formerly known as Knowledge Base articles.
Forums on the SAP Community Network	https://www.sdn.sap.com/irj/scn/forums
Training	https://training.sap.com From traditional classroom learning to targeted e-learning seminars, we can offer a training package to suit your learning needs and preferred learning style.
Online customer support	http://service.sap.com/bosap-support The SAP Support Portal contains information about Customer Support programs and services. It also has links to a wide range of technical information and downloads. Customers with a maintenance agreement have an authorized user ID to access this site. To obtain an ID, contact your customer support representative.
Consulting	http://www.sap.com/services/bysubject/businessobjectsconsulting Consultants can accompany you from the initial analysis stage to the delivery of your deployment project. Expertise is available in topics such as relational and multidimensional databases, connectivity, database design tools, and customized embedding technology.

Index

.NET

- BusinessObjects Enterprise .NET SDK 97
- Crystal Reports .NET SDK 98
- Report Application Server (RAS) .NET SDK 98
- Report Engine .NET SDK 98
- .NET web application servers 97

A

- access 708
 - applications 774
 - calendars 894
 - categories 910, 912
 - CMC 774
 - events 899
 - folders 907
 - groups 765
 - inboxes 765
 - InfoView 774
 - profiles 965
 - Query HTML panel 780
 - server groups 181
 - servers 181
 - universe connections 787
 - users 765
- access control lists
 - adding principals to 722
 - viewing 720
- access levels 709, 719, 740
 - administration 740
 - assigning to principals 722
 - copying 733
 - creating 733
 - deleting 734
 - access levels (*continued*)
 - managing across sites 736
 - modifying rights in 734
 - predefined 728
 - RAS 182
 - relationships to objects 736
 - renaming 733
 - rights 1008
 - tasks, rights required for 728
 - view vs. view on demand 731
 - viewing 720
 - when copying/moving folders 905
- accounts, managing 748, 753
- active sessions, viewing 535
- active trust relationship 137
- Adaptive Processing Server 74
- adding 241
 - cluster members 241
 - CMS 243
 - Crystal reports 914
 - objects 914
 - to categories 919
 - to object packages 833, 926
 - with CMC 926
 - with Publishing Wizard 915
 - servers 174
 - subgroups 758
 - users to groups 760
- administration 700
 - applications 774
 - categories 912
 - CMC 774
 - configuration tools 150, 532
 - delegating 740
 - events 899
 - folders 907

Index

administration (*continued*)

- groups 765
- inboxes 765
- InfoView 774
- profiles 965
- rights 740
- servers and server groups 181
- tools 700
- users 765

Administrator account, setting password 705

adopting nodes 165

advanced rights 709, 719, 722

affinity, and SSL 138

alerts, setting notification 851

aliases

- assigning to users 769
- creating 768
 - for existing users 768
 - for new users 767
- deleting 769
- disabling 770
- managing 767

anonymous single sign-on 132

application settings for Content Search 980

application tier 183

apsdbsetup.sh 680

architecture 36

architecture diagram 38

areas, management 702

assigning

- aliases 769
- objects to categories 797

attributes, logon tokens 137

audit notification 849

auditing 574

- auditee 568
- auditor 568
- configuring database 574
- database schema 620
- detail codes 625
- enabling 593
- event codes 625

auditing (*continued*)

- information flow 568
- optimizing performance 601
- publication destinations 592
- Publishing 592
- report names 607
- reporting results 599, 620
- synchronizing records 600
- user and system events 577
- web activity 141

auditing database 104, 574

- configuring 574
- database schema 620
 - Application_Type table 624
 - Audit_Detail table 621
 - Audit_Event table 620
 - Detail_Type table 624
 - Event_Type table 623
 - Server_Process table 622

authentication 105, 107, 135

- LDAP 275, 276
- object packages 835
- primary 128
- security plug-ins 134
- Trusted Authentication 371, 763
- types 751
- Web Application Container Server (WACS) 489
- Windows AD 294
- Windows NT 264

authorization 107

automatic

- categorization 973
- starting servers 171

B

backing up

- server configuration settings 247

BI Widgets, rights 1036

Business Objects inboxes

- sending publications to 945

- Business Process BI Service 61
- Business View Manager 53
- BusinessObjects Enterprise
 - architecture diagram 38
 - communication between servers 444
 - deployment with reverse proxy servers 510, 511
 - documentation 32
 - primary authentication process 128
 - rights 708
 - scalability 553
 - security settings 705
 - single sign-on 135
 - top-level folders, rights 723
 - Web Application Container Server (WACS) 470
 - what's new 27
- BusinessObjects Enterprise .NET SDK 97
- BusinessObjects Enterprise Java SDK 94
- BusinessObjects Enterprise SDK 136, 813
- BusinessObjects Enterprise servers
 - configure Kerberos and browsers 315, 491
 - configuring hosts file for firewall 460
- BusinessObjects Enterprise Sizing Guide 553
- BusinessObjects Mobile 49

C

- cacert.der 236
- cache format, Web Intelligence documents 875
- Cache Server 656
 - command-line options 656
 - configuring 552
 - for viewing reports 804
 - metrics 535
 - performance settings 552
- cakey.pem 236
- calendars 887
 - adding dates to 888
 - adding specific dates 890
 - creating 887
 - deleting 893
- calendars (*continued*)
 - format options 889
 - recurring dates 891
 - specifying rights 894
- categories 903
 - adding a report 911
 - adding objects to 919
 - assigning objects to 797
 - creating 909
 - deleting 910
 - moving 910
 - removing/deleting objects 911
 - rights 912, 1000
- CCM
 - adding a server 174
 - adding nodes 163
 - changing
 - server user account 227
 - command-line options 655
 - deleting a server 177
 - enabling and disabling servers 172
 - for UNIX 674
 - nodes 162
 - recreating existing nodes 166
 - Server Intelligence Agent 158
 - server management 158, 159
 - servers 158
 - starting, stopping, and restarting servers 168
- ccm.sh 674
- Central Configuration Manager (CCM) 54
- Central Management Console (CMC) 50
 - clustering 40
 - fault tolerance 40
 - load balancing 40
 - session affinity 40
- Central Management Console Service 62
- Central Management Server (CMS)
 - security 105
- Central Management Service 62
- Central Management System (CMS)
 - database 102

Index

- certificate files 236, 484
- certificate trust lists 485
- characters, setting CMC preferences 702
- checking, relationships between objects 797, 798
- client 48
- Client Auditing Proxy Service 62
- clients, browser-based 49
 - BusinessObjects Mobile 49
 - Central Management Console (CMC) 50
 - Dashboard and Analytics 50
 - InfoView 51
 - Report viewers 51
 - Server Intelligence 46
 - Voyager 52
 - Web Intelligence 53
- clients, desktop 53
 - Business View Manager 53
 - Central Configuration Manager (CCM) 54
 - Crystal Reports Designer 54
 - Crystal Reports Viewer 54
 - Data Source Migration Wizard 55
 - Desktop Intelligence 55
 - Import Wizard 55
 - Live Office 56
 - Publishing Wizard 56
 - Query as a Web Service 57
 - Report Conversion Tool 57
 - Repository Diagnostic Tool 58
 - Translation Manager 58
 - Universe Builder 59
 - Universe Designer 59
 - Web Intelligence Rich Client 60
 - Xcelsius 60
- cloning
 - servers 175
 - Web Application Container Servers (WACS) 480
- clustering
 - support 40
- clusters 241, 243
 - adding a CMS 243
 - clusters (*continued*)
 - adding nodes 163
 - adopting nodes 166
 - changing names 245
 - nodes 162, 241
 - viewing details 541
 - CMC
 - adding to a Web Application Container Server (WACS) 481
 - cloning servers 175
 - controlling access to 774
 - creating publications in 953
 - deleting a server 177
 - enabling and disabling servers 172
 - logging on 701
 - management areas 702
 - managing servers 152
 - navigating 702
 - removing default servers 165
 - removing from a Web Application Container Server (WACS) 482
 - rights 1012
 - setting preferences 702
 - starting, stopping, and restarting servers 168
 - Windows server dependencies 227
 - CMS
 - adding to a cluster 243
 - as nameserver 194
 - authentication 128
 - changing cluster name 245
 - clustering 241
 - installing new cluster member 243
 - requirements 241
 - command-line options 650
 - configuring 194, 206, 209
 - default port 194
 - distributed security 138
 - enabling and disabling other servers 172
 - metrics 535, 541
 - saving objects to 929

- CMS (*continued*)
 - session variables 139
 - authentication 128
 - tracking 140
 - starting 171
 - stopping 171
 - troubleshooting 171
 - troubleshooting multihomed machines 194
- CMS clusters
 - adding to web.xml 244
- CMS system database 209
 - changing password 209
 - configuring 198
 - copying 198
 - deleting 206
 - recreating 206
 - selecting 209
- command line arguments, specifying 824, 926
- command-line options 646, 666, 671
 - all servers 647
 - Cache Server 656
 - CCM 655
 - CMS 650
 - Event Server 671
 - Input and Output File Repository Servers 668
 - Job Server 659
 - Processing Server 656
 - Program Job Server 659
 - Report Application Server 662
 - SSL 235
 - standard options 647
 - Web Intelligence Job Server 659
- communication 128
 - between browser and Web application server 128
 - between BusinessObjects Enterprise servers 444
- configuration templates 184
 - applying 186
 - best practices 184
 - restoring system defaults 187
- configuration templates (*continued*)
 - setting 185
- configuring 574
 - Apache 2.2 515
 - application tier 183
 - auditing database 574
 - on UNIX 577
 - on Windows 576
 - auditing universe connection 598
 - Cache Server 552
 - clusters 241
 - CMS clusters 245
 - CMS database 209
 - CMS system database 198, 206
 - configuration templates 185
 - Crystal Reports Processing Server 219
 - Event Server 551
 - executable programs 826
 - File Repository Servers 211, 552
 - firewalls 457
 - intelligence tier 183
 - ISA 2006 517
 - Java programs 828
 - Job Server 212, 219
 - multiple servers 184
 - nodes 241
 - object packages 834
 - Processing Server 212
 - processing tier 183
 - reverse proxy servers 512
 - servers 150, 532
 - Trusted Authentication 372, 373
 - WebSEAL 6.0 516
- Connection Server
 - metrics 535
- Connection Service 68
- Content Search 968
 - application settings 980
 - concurrent indexing 983
 - creating the initial index 988
 - disabling 984
 - disk space 979

Index

- Content Search (*continued*)
 - estimating user load 978
 - exclude objects 976
 - facets 973
 - index location 982
 - indexing failure 992
 - indexing program, managing 988
 - indexing schedule 990
 - initial indexing 987
 - installation and upgrade 980
 - instances 973
 - JVM heap size 986
 - limits on search results 976
 - locks 993
 - Maximum group instances indexed 985
 - memory 979
 - multilingual search 972
 - objects types 968
 - parameters and prompts 973
 - processors 979
 - rebuild index 981
 - reports with view time security 974
 - rights 984, 991
 - security considerations 976
 - servers and architecture 977
 - set search language 982
 - suggested queries 975
 - syntax and interpretation 970
 - terminating the indexing process 991
- cookies 139
 - logon tokens 137
 - session tracking 139
- copying
 - access levels 733
 - folders 905
 - objects 790
- creating
 - access levels 733
 - categories 909
 - custom auditing reports 620
 - folders 903
 - groups 756
 - creating (*continued*)
 - initial indexes, Content Search 988
 - object packages 833
 - object shortcuts 791
 - profiles 957
 - publications
 - in CMC 953
 - in InfoView 953
 - server groups 178
 - server subgroups 179
 - user accounts 754
- Crystal reports
 - adding 914
 - adding with existing hyperlinks 819
 - database settings 806
 - job server for scheduling 804
 - processing extensions 814
 - Publishing formats 949
 - refresh options 800
 - rights 1002
 - sample auditing reports 599
 - scheduling format options 869
 - specifying parameters for 807
 - using filters for 809
 - viewing options 802
- Crystal Reports .NET SDK 98
- Crystal Reports Cache Server
 - metrics 535
- Crystal Reports Cache Service 66
- Crystal Reports Designer 54
- Crystal Reports Processing Server 656
 - command-line options 656
 - configuring on UNIX 220
 - metrics 535
 - performance settings 212
 - Properties page 212
- Crystal Reports Processing Service 66
- Crystal Reports Scheduling Service 67
- Crystal Reports Viewer 54
- Crystal Reports Viewing and Modification Service 67
- CSV, scheduling format options 869

- custom auditing report creation 620
- custom events 894, 898
- custom web applications, enhancing 557

D

- daemons, signal handling 650
- Dashboard and Analytics 50
- dashboards, rights 1008
- data
 - live 731
 - saved 731
- data refresh 937
- data sharing 150, 532
 - on Cache Server 552
 - on Processing Server 212
- data source connections 786
- Data Source Migration Wizard 55
- data sources 220
 - on UNIX 220
 - on Windows 219
- database fetches 937
- databases 102
 - auditing 104
 - Central Management System (CMS) 102
 - changing settings 806
 - configuring servers for 219
 - copying CMS data 198
 - initializing the CMS 206
 - selecting for the CMS 209
 - single sign-on access 133
 - universe 103
 - views 104
- default servers in new node 165
- default settings 135
 - authentication 135
 - Enterprise accounts 135
 - ports 194
 - security plug-in 135
 - servers 187
- delegated administration 740
- deleting 206
 - access levels 734
 - aliases 769
 - categories 910
 - CMS system database 206
 - folders 903
 - groups 759
 - objects 792
 - servers 177
 - servers from new node 165
 - subfolders 904
 - universe connections 787
 - universes 787
 - user accounts 755
 - Web Application Container Servers (WACS) 481
- delivery rules 939
- deployment
 - documentation 32
- DES encryption 305
- Designer, rights 1035
- Desktop Intelligence 55
 - rights 1015
- Desktop Intelligence Cache Service 68
- Desktop Intelligence documents
 - Publishing formats 949
 - rights 1003
 - updating prompts 808
- Desktop Intelligence Processing Service 69
- Desktop Intelligence Scheduling Service 69
- Destination Delivery Scheduling Service 63
- Destination Job Server 213
 - destinations 213
 - configuring 213
 - enabling or disabling 213
- destination sites
 - access levels 736
- destinations
 - available, by object type 795
 - default settings 854
 - email 860

Index

- destinations (*continued*)
 - for job servers 213
 - configuring 213
 - enabling or disabling 213
 - FTP 858
 - inbox 863
 - publications 943, 945
 - scheduling 853
 - sending to 793
 - unmanaged disk 855
 - diagram, architecture 38
 - directory servers 276
 - about LDAP 277
 - security plug-in 276
 - disabling
 - aliases 770
 - Content Search 984
 - destinations for job servers 213
 - Guest account 706
 - guest accounts 759
 - servers 172
 - discussion threads 775
 - cancelling search 775
 - right to add 779
 - searching 775
 - sorting search results 777
 - Discussions 779
 - disk space required for Content Search 979
 - DLL 136, 813
 - secEnterprise.dll 135
 - secLDAP.dll 276
 - secWindows.dll 264
 - document types, Publishing 933
 - DSNs on UNIX 222
 - dynamic recipient sources 942
 - dynamic recipients 942
 - dynamic-link libraries, processing extensions 136, 813
 - email destination
 - scheduling objects to 860
 - sending publications to 945
 - setting defaults 215
 - email notification 849
 - enabling
 - auditing 593
 - destinations for a job server 213
 - servers 172
 - encoding, logon tokens 137
 - end-to-end single sign-on 134
 - Enterprise locations, publications 945
 - env.sh 684
 - environment variables 222
 - ODBC 222
 - specifying for program objects 827
 - estimating user load, Content Search 978
 - Event Log 227, 542
 - Event Server
 - command-line options 671
 - configuring 551
 - metrics 535
 - polling time 551
 - Event Service 63
 - events
 - access to 899
 - custom 898
 - file-based 895
 - managing 894
 - notification 849
 - polling time 551
 - schedule-based 897
 - scheduling 845
 - Excel, scheduling format options 869
 - excluding, objects from Content Search 976
 - executable programs 822
 - configuring 826
 - exporting, objects to CMS 929
 - extensions, processing 136, 813
 - external recipients 942
- E**
- effective rights 719

F

- facets and labels 973
- fault tolerance
 - session affinity
 - web application support 40
- support 40
- Favorites folders 909
- federation 382
 - access levels 736
 - benefits 382
 - best practices 432
 - enhancing performance 436
 - importing and promoting replicated content 429, 430, 431
 - locally run instances 425
 - managing conflicts 416
 - managing security 403
 - object cleanup 410
 - one-way replication 413
 - refresh from destination 413
 - refresh from origin 413
 - remote connections 394
 - creating 394
 - modifying 396
 - remote scheduling 425
 - replicating large objects 432
 - replication jobs 397
 - creating 398
 - modifying 401
 - scheduling 401
 - replication lists 387
 - creating 388
 - folders 388
 - managing 393
 - replication modes 413
 - repointing destination sites 429, 431
 - terms 384
 - third-party users and groups, replicating 408
 - troubleshooting 437
 - two-way replication 413
 - viewing logs 402
- federation (*continued*)
 - web services 423
- file events 894, 895
- File Repository Servers
 - command-line options 668
 - maximum idle times 211, 552
 - metrics 535
 - Properties page 211, 552
 - root directories 211, 552
- file system destination
 - setting defaults 218
- filtering, publication data 951
- filters, for Crystal reports 809
- firewalls 141
 - configuration scenarios 461
 - configuring 457
 - forcing servers to register by name 197
 - server communications, and 444
 - Web Application Container Server (WACS) 500
- folder inheritance 713
 - rights override 714
- folders 902
 - adding a report 906
 - copying/moving 905
 - creating 903
 - default user folders 909, 912
 - deleting 903
 - Favorites folder 909
 - object rights
 - inheritance 713
 - rights 907, 1000
 - setting instance limits 907
- formats
 - publications 948, 949
- FTP destination
 - for publications 945
 - for scheduling 858
 - setting defaults 217

Index

G

- global profile targets 958, 959
- global system metrics 541
- groups
 - adding subgroups 758
 - adding users to 760
 - assigning rights to 722
 - checking rights for 724, 725
 - creating 756
 - default 749
 - deleting 759
 - granting access to 765
 - managing 749
 - modifying 756
 - rights 1006
 - breaking inheritance 738
 - inheritance 711
 - on top-level folders 723
 - rights override 714
 - setting instance limits on folders 907
 - specifying group membership 758
 - viewing
 - members 757
 - rights for 720
- Guest accounts
 - disabling 706, 759

H

- high-volume publications 937
- hosts
 - configuring LDAP 280
- hosts file, configuring for NAT firewall 460
- HTTP 128, 139
- HTTPS
 - configuring Web Application Container Servers (WACS) 483, 486, 499
- hyperlinks, between reports 818

I

- idle times 552
 - Cache Server 552
 - File Repository Servers 211, 552
 - Processing Server 212
- IIS
 - database single sign-on configuration 355, 356, 357
- Import Wizard 55
- importing
 - nodes 247
 - server configuration settings 247
- inactive clusters 165
- inboxes
 - controlling access to 765
 - scheduling objects to 863
- incremental indexing 990
- index location, Content Search 982
- index, setting CMC preferences 702
- indexing failure, Content Search 992
- indexing program, Content Search 988
 - object rights 991
- indexing schedule, Content Search 990
- InfoView 51
 - accessing 701
 - categories 912
 - clustering 40
 - controlling access to 774
 - creating publications in 953
 - fault tolerance 40
 - folders 909
 - Java version 779
 - load balancing 40
 - logon 765, 766
 - managing 779
 - rights 1013
 - session affinity 40
- inheritance 710
 - breaking 738
 - folder 713
 - group 711

- inheritance (*continued*)
 - limiting 716
 - rights override 714
- initial indexing, Content Search 987
- initializing CMS system database 206
- initlaunch.sh 686
- Input File Repository Server
 - configuration 201
 - maximum idle time 211, 552
 - metrics 535
 - root directory 211, 552
- Input Filestore Service 63
- installation and upgrade, Content Search 980
- Instance Manager 881
- instance share 425
- instances 885
 - columns 884
 - deleting 885
 - finding 882
 - managing 878, 880, 881
 - notification 849
 - object 799
 - object packages 832
 - pausing 884
 - program objects 822
 - report objects 799
 - resuming 884
 - scheduled 799
 - search with Content Search 973
 - sending 793
 - setting limits at the folder level 907
 - viewing 884
- intelligence tier 183
- IPv6
 - CMC 188
 - options 188
 - setting address in CMC 191
- ISA 2006
 - configuring for Oracle 10gR3 524
 - configuring for Sun Java 8.2 524
 - configuring for Tomcat 5.5 524
 - configuring for WebSphere CE 2.0 524

J

- JAAS, configuration file 318, 319, 493
- Java
 - BusinessObjects Enterprise Java SDK 94
 - JavaServer Faces (JSF) SDK 96
 - Report Application Server (RAS) Java SDK 95
 - Report Engine Java SDK 95
 - Viewers Java SDK 95
- Java application server, Kerberos 315
- Java programs 822
 - configuring 828
 - JVM arguments 828
 - providing access to other files 828
 - setting parameters 828
- Java web application servers 94
- Java, Kerberos 320, 321, 322
- JavaServer Faces (JSF) SDK 96
- Job Server 219, 659
 - command-line options 659
 - configuring 219
 - configuring, on UNIX 220
 - destinations 213
 - configuring 213
 - enabling or disabling 213
- JVM heap size 986

K

- Kerberos 315, 491
 - configuration file 315, 317, 492
 - Krb5.ini 319, 493
 - single sign-on for Java 350
 - single sign-on for Java InfoView 330
 - troubleshooting 327, 495
- Kerberos configuration 304
 - IIS 313
 - Oracle 313
 - Tomcat 312
 - WebLogic 313
 - WebSphere 313

Index

key files 236
Krb5.ini 319, 493

L

LDAP

- accounts 275, 277
 - modifying connection parameters 290
 - modifying member groups 290
 - troubleshooting 294
- authentication 275
 - configuring 280
- authentication plug-in 276
- configuring single sign-on 291
- groups
 - mapping 287
 - unmapping 289
 - viewing 289
- hosts
 - configuring 280
 - managing multiple 284
- managing 275
- mapping against Windows AD 278
- Secure Sockets Layer (SSL) 277
- security plug-in 276

license keys 146

- adding 146
- and CMS database migration 204
- reinitializing the CMS system database 206
- viewing account activity 147

licensing, accessing information 146

Life Cycle Management (LCM) 47

Life-Cycle Management (LCM)

- Life-Cycle Manager 47

Lightweight Directory Access Protocol. *See* LDAP 277

limiting

- folder level instances 907
- scope of rights 716
- search results, Content Search 976

List of Values Job Server

- destinations 213
 - configuring 213
 - enabling or disabling 213

List of Values Scheduling Service 67

live data 731

Live Office 56

- configuration for reverse proxy servers 521

load balancer

- support 40

load balancers 56

load balancing 138

- adding a CMS 243
- and distributed security 138
- clustering 241
- Web Application Container Servers (WACS) 498

local disk 945

local profile targets 958

Local System account 219

locks, Content Search 993

log on 219

- InfoView 766
- processing server accounts 219
- protection against malicious attempts 141
- to the CMC 701

logging 542

- server activity 542
- web activity 141
- Web Application Container Server (WACS) 501

logon tokens 137

- authentication 128
- distributed security 138
- session tracking 139

logon.csp 128

M

management areas 702

management services 41

- managing applications 774, 782
 - Discussion threads, deleting 778
 - Discussions settings 775
- mapped users, managing aliases 767
- Maximum group instances indexed, Content Search 985
- memory settings
 - changing on a Web Application Container Server (WACS) 506
- memory, required for Content Search 979
- menu styles, setting CMC preferences 702
- metrics 147
 - viewing 534
 - viewing account activity 147
- Microsoft Excel, scheduling format options 869
- Microsoft Word, scheduling format options 869
- migrating, CMS system database 198
- moving, objects 791
- Multi-Dimensional Analysis Server 84
- Multi-Dimensional Analysis Service 70
- multihomed machines 191
 - Web Application Container Server (WACS) 500
- multilingual search 972
- multiple documents, Publishing 933

N

- native drivers 219
 - on UNIX 220
- navigation
 - between reports 818
- navigation tree
 - servers 152
- Network Address Translation
 - configuring, server hosts file 460
- network interface
 - troubleshooting multiple 193
- networking environments
 - IPv4
 - dual IPv4/IPv6 nodes 188
 - IPv6 188
- new features 27
- nodes 60, 162
 - adding 163
 - a CMS 243
 - to a cluster 243
 - to an inactive cluster 165
 - adopt 166
 - clustering 241
 - CMC 152
 - recreating a SIA 165
 - removing extra servers 165
- nodes importing 247
- non-primary network interface 193
- notes, rights 1001
- notifications
 - alerts 851
 - audit 849
 - email 849
 - event 849
 - for a scheduled object 847
 - object's failure, success 847
- number of logons, logon tokens 137
- number of minutes, logon tokens 137

O

- object conflicts
 - one-way replication 416
 - two-way replication 416
- object instances 799
- object packages 833, 917
 - adding objects to 833, 926
 - authentication 835
 - configuring 834
 - creating 833, 917
 - instances 832
 - managing 832
 - moving objects between 918
 - scheduling 844
- object rights
 - general 996
 - when moving categories 910

Index

- object shortcuts 791
- object types, for Content Search 968
- objects
 - adding
 - Crystal reports 914
 - multiple 915
 - to an object package 833
 - with CMC 926
 - with saved data 921
 - categories
 - adding to 919
 - assigning to 797
 - changing
 - default settings 799
 - properties 796
 - copying 790
 - creating shortcuts to 791
 - deleting 792
 - exporting to CMS 929
 - failure notification 847
 - format 864
 - managing 790
 - moving 791
 - rights
 - setting 722
 - viewing 720
 - rights, general 996
 - saving to CMS 929
 - scheduling
 - recurrence pattern 839
 - with Publishing Wizard 920
 - searching for 792
 - sending 793
 - success notification 847
- objects per page, setting maximum 702
- ODBC
 - CMS database
 - connectivity 204
 - drivers 219
 - environment variables 222
 - processing server accounts 219
 - reporting on UNIX 222

- ODBC (*continued*)
 - system information file 222
- odbc.ini 222
- one-way replication 413
- Oracle
 - JAAS 318
 - Java options 321
 - Kerberos 315
- organizing, objects 902
- origin sites
 - access levels 736
- Output File Repository Server
 - configuration 201
 - maximum idle time 211, 552
 - metrics 535
 - root directory 211, 552
- Output Filestore Service 64
- owner rights 744

P

- page index, setting CMC preferences 702
- pages, setting CMC preferences 702
- parameters
 - and Content Search 973
 - for Java programs 828
 - for report objects 807
- passwords 209
 - changing 761
 - for CMS database 209
 - options 762
 - restrictions 142
 - setting 705
 - CMC preferences 702
 - for Administrator account 705
 - for current CMC user 702
- patchlevel.sh 685
- PDF, scheduling format options 869
- performance 553, 601
 - assessment 532
 - Cache Server settings 552
 - clusters 241

- performance (*continued*)
 - general considerations 554
 - load balancing 138
 - troubleshooting 544
 - while auditing 601
- Performance Management
 - rights 1024
- Permissions Explorer 720
- personal categories 912
- personalizing
 - publications 951
- plain text, scheduling format options 869
- plug-ins
 - security 106
- plug-ins, security 134
- Polestar 782
 - application properties 782
 - managing settings 782
 - rights 1037
- port numbers
 - changing 194
 - conflicts 504, 505
 - Web Application Container Server (WACS) 503
- postinstall.sh 686
- preferences, setting in the CMC 702
- primary authentication 128
- primary network interface 193
- principals
 - assigning advanced rights to 722
 - assigning rights to 722
 - checking rights for 724, 725
 - rights, on top level folders 723
 - viewing rights for 720
- printing
 - assigning printers 811
 - Crystal reports 810
- processing extensions 136, 813
 - applying to reports 814
 - registering 815
 - selecting 817
 - sharing 818
- Processing Server
 - command-line options 656
 - configuring 220
 - configuring for data source 219
 - for viewing and modifying 804
 - Web Intelligence 666
- processing services 43
- processing settings 877
- processing threads 552
 - Cache Server 552
 - Processing Server 212
- processing tier 183
- processors, for Content Search 979
- profile targets 958
- profile values 958
 - conflicts 964
 - types 960
 - variable 962
- profiles 956
 - access to 965
 - conflicts 963
 - creating 957
 - global profile targets, specifying 959
 - profile targets 958
 - profile values 958
 - conflicts 964
 - types 960
 - variables 962
 - role in Publishing 957
- program credentials, specifying 923
- Program Job Server 213
 - command-line options 659
 - destinations 213
 - configuring 213
 - enabling or disabling 213
- program objects 822, 925
 - access to other files 925
 - adding, with Publishing Wizard 922
 - authentication 829, 831
 - batch 922
 - binary 922
 - command line arguments 926

Index

- program objects (*continued*)
 - enabling, disabling 829, 831
 - environment variables, specifying 827
 - executable programs, configuring 826
 - file access to executable programs 826
 - Java programs 828
 - managing 822
 - script 922
 - working directory, specifying 824
- Program Scheduling Service 64
- prompts
 - and Content Search 973
 - updating
 - for Desktop Intelligence documents 808
 - for Web Intelligence documents 808
- publications 933
 - creating
 - in CMC 953
 - in InfoView 953
 - delivery rules 939
 - destinations 943, 945
 - dynamic recipients 942
 - formats 948, 949
 - multiple documents 933
 - personalization 951
 - report bursting 937
 - subscribing and unsubscribing 952
- Publishing 932
 - administration recommendations 560, 561
 - auditing 592
 - deployment configuration recommendations 561
 - destinations
 - auditing 592
 - profiles, role of 957
 - rights required 935
 - workflow 934
- Publishing Post Processing Service 64
- Publishing Service 65
- Publishing Wizard 56, 915
 - choosing
 - folders 916

- Publishing Wizard (*continued*)
 - choosing (*continued*)
 - objects 916
 - creating
 - category on CMS 919
 - folder on CMS 917
 - database logon 924
 - default values, modifying 923
 - duplicating folder structure 918
 - logging on to 915
 - moving objects between folders 918
 - program objects
 - adding extra files 925
 - command line arguments 926
 - types 922
 - repository refresh 921
 - scheduling
 - formats 925
 - objects 920
 - selecting
 - category on CMS 919
 - folder on CMS 917
 - setting parameters 924
- punctuation in Content Search 970

Q

- queries
 - relationships 797, 798
 - security 724, 725
- Query as a Web Service 57, 100
- Query as a Web Service (QaaWS) Service 65
- Query HTML panel, access rights 780

R

- rebuild Content Search index 981
- recipients
 - dynamic 942
 - personalizing publications for 951
- recovery 166
- recurrence patterns, object scheduling 839

- refresh mode options, for federation 413
- refreshing 552
 - cache files 552
 - reports 800
 - source document data 937
- registry keys 292
- relationship queries 797, 798
 - for access levels 736
- relationships 797, 798
- remote connections
 - creating 394
 - creating folders 394
 - modifying 396
 - security 396
 - viewing 394
- Remote Procedure Call 227
- remote scheduling 425
- renaming, access levels 733
- replicating
 - objects 382
 - third-party users and groups 408
- replication jobs
 - configuration options 398
 - creating 398
 - modifying 401
 - scheduling 401
 - viewing 397
- replication lists
 - creating 388
 - dependency options 388
 - managing 393
 - modifying 393
 - supported objects 387
- Replication Service 65
- Report Application Server 804
 - command-line options 662
 - metrics 535
 - required object rights 182
- Report Application Server (RAS) .NET SDK 98
- Report Application Server (RAS) Java SDK 95
- report bursting 937
- Report Conversion Tool 57
- Report Engine .NET SDK 98
- Report Engine Java SDK 95
- report instances
 - columns 884
 - history 879
 - managing 799, 880
 - setting limits 885
 - viewing 884
- report objects
 - adding
 - with existing hyperlinks 819
 - adding and hyperlinking 821
 - adding to a folder individually 906
 - database settings, specifying 806
 - destination 853
 - filters, specifying 809
 - hyperlinking 818
 - hyperlinks, viewing 820
 - managing 799
 - parameters, specifying 807
 - processing extensions 814
 - refresh options 800
 - rights 1002
 - rights for creating/modifying 182
 - scheduling with events 845
 - setting instance limits 885
 - specifying Job Servers for 804
 - specifying servers 804
 - viewing options 802
- report thumbnails, adding with reports 906, 911
- Report Viewers 51
- reports 599, 911
 - adding to a category individually 911
 - auditing 599, 620
 - custom 620
 - sample 599
 - configuring servers for data sources 219
- Repository Diagnostic Tool 58
- requirements
 - clustering 241
- restart.sh 684
- restarting servers 168

Index

- restore
 - system defaults 187, 507
- restoring
 - server configuration settings 247
- restrictions 143
 - guest account 143
 - logon 142
 - password 142
 - user 143
- reverse proxy servers
 - BI web services 529
 - configuring Apache 2.2 515
 - configuring ISA 2006 517
 - configuring WebSEAL 6.0 516
 - configuring with BusinessObjects Enterprise 512
 - deployment with a Web Application Container Server (WACS) 499
 - deployment with BusinessObjects Enterprise 510, 511
 - Live Office 528
 - session cookies 524
 - special configuration 521
 - Tomcat 521
 - using with Web Application Container Servers (WACS) 499
 - viewer URL 528
 - web services 521
- rich text, scheduling format options 869
- rights 708, 996
 - access levels 709, 1008
 - managing across sites 736
 - modifying included rights 734
 - relationship queries 736
 - replicated 736
 - tasks 728
 - administration 740, 745
 - advanced rights 709, 722
 - applications 774
 - assigning to principals 722
 - BI Widgets 1036
 - calendars 894
 - categories 912, 1000
 - CMC 774, 1012
 - Content Search 984
 - Crystal reports 1002
 - dashboards 1008
 - Designer 1035
 - Desktop Intelligence 1015
 - Desktop Intelligence documents 1003
 - effective rights 719
 - events 899
 - folders 907, 1000
 - general 996
 - groups 765, 1006
 - inboxes 765
 - InfoView 774, 1013
 - inheritance 710
 - breaking 738
 - folder 713
 - group 711
 - limiting scope of 716
 - managing 720
 - managing security 403
 - notes 1001
 - owner rights 744
 - Performance Management 1024
 - Polestar 1037
 - profiles 965
 - Report Application Server 182
 - requirements, for Publishing 935
 - rights
 - replicating 403
 - rights override 714
 - scope of rights 716
 - security query 724, 725
 - server groups 181
 - servers 181
 - Strategy Builder 1034
 - top-level folders 723
 - type-specific 717
 - universe connections 1012
 - universes 1009

- rights (*continued*)
 - users 765, 1006
 - view vs. view on demand 731
 - viewing 720
 - Web Intelligence 1020
 - Web Intelligence documents 1004
 - when copying/moving folders 905
- root directories, File Repository Servers 211, 552
- row-level security, processing extensions 136, 813
- Run Now 900
- run options, object scheduling 841

S

- sample auditing reports 599
- saved data 731
 - adding objects with 921
- saving, objects to CMS 929
- schedule events 894, 897
- scheduled instances 799
- scheduling 838, 847
 - events 845
 - formats 869
 - increasing capacity 555
 - notification 847
 - object packages 844
 - objects 843, 847
 - for group 876
 - for user 876
 - in batches 844
 - recurrence patterns 839
 - run options 841
 - recurrence patterns 838
 - Run Now 900
 - server group settings 877
 - setting for an object 847
 - specifying server for 804
 - with Publishing Wizard 920
- scope of rights 716
- script programs 822
- SDK
 - web services 99
- search
 - facets, Content Search 973
 - instances, Content Search 973
 - multilingual 972
 - parameters and prompts, Content Search 973
 - reports with view time security, Content Search 974
 - syntax and interpretation, Content Search 970
- Search Service 65
- searchable objects, Content Search 968
- searching 775
 - discussion threads 775
 - for objects 792
- Secure Sockets Layer (SSL) 140, 235, 277
 - and LDAP 277
 - and load balancing 138
- security 105, 126
 - active trust relationship 137
 - auditing web activity 141
 - Central Management Server (CMS) 105
 - distributed 138
 - environment protection 140
 - firewalls 141
 - Guest account restrictions 143
 - initial settings 705
 - logon restrictions 142
 - managing 720
 - password restrictions 142
 - plug-ins 106, 134
 - processing extensions 136, 813
 - protection against malicious logon attempts 141
 - queries 724, 725
 - restrictions 143
 - session tracking 139
 - top level folders 723
 - universe objects 1011
 - user restrictions 143

Index

security (*continued*)

- web browser to web server 140
- web servers 140

security plug-ins 134

- Enterprise authentication 135
- LDAP authentication 276
- Windows AD authentication 296
- Windows NT authentication 264

sending

- instances 793
- object shortcuts 793
- to destinations 793
- to inboxes, default configuration 213

separated values, scheduling format options 869

Server cache expiry, modifying default expiry value 326

server groups

- access to 181
- creating 178
- nodes 152
- subgroups 179
- subgroups of servers 178

Server Intelligence 46, 158

Server Intelligence Agent

- adding 163
- changing
 - server user account 227
- dependencies
 - adding or removing 227
- nodes 162
- recreating 166
- removing default servers 165
- starting servers automatically 171

Server Intelligence Agent (SIA) 158

server management 158

- differences in versions 159

server properties 1042

server states 152

serverconfig.sh 680

servers 150, 532

- access to 181

servers (*continued*)

- activity, logging 542
- Adaptive Job Server 73
- Adaptive Processing Server 74
- adding 174
- Central Management Server 74
- changing 167
 - status 167
 - user account on Windows 227
- changing dependencies 227
- cloning 175
- command lines 646
- Common Server Settings
 - Auto Assign 1042
 - Automatically start this server when the SIA starts 1042
 - Host Identifiers 1042
 - Request Port 1042
 - Restore System Defaults 1042
 - Set Configuration Template 1042
 - Use Configuration Template 1042
- communication 444
- configuration templates 184
 - applying 186
 - setting 185
- configuring 150, 183, 532
- configuring servers to use service account 311
- configuring tracing 232
- Connection Server 76
- contrast with services 60
- Core Server Settings
 - Bind to All IP Addresses 1044
 - Bind to Hostname or IP Address 1044
 - bscLogin.conf File Location 1044
 - Certificate Alias 1044
 - Certificate Store File Location 1044
 - Certificate Store Type 1044
 - Certificate Trust List File Location 1044
 - Certificate Trust List Private Key Access Password 1044
 - Cleanup Interval 1044

servers (*continued*)Core Server Settings (*continued*)

- Disable Auto Reconnect to System and Auditing Databases 1044
- Enable Client Authentication 1044
- Enable HTTP through Proxy 1044
- Enable HTTPS 1044
- Event Poll Interval 1044
- File Store Directory 1044
- HTTP Port 1044
- HTTPS Port 1044
- Krb5.ini File Location 1044
- Log level 1044
- Maximum Concurrent Jobs 1044
- Maximum Concurrent Requests 1044
- Maximum Idle Time 1044
- Maximum Retries for File Access 1044
- Maximum size of the thread pool 1044
- Name Server Port 1044
- Private Key Access Password 1044
- Protocol 1044
- Proxy Hostname 1044
- Proxy Port 1044
- Service Startup Timeout 1044
- Single Sign-On Expiry 1044
- System Database Connections Requested 1044
- Temporary Directory 1044
- Crystal Reports Cache Server 77
- Crystal Reports Processing Server 77, 91
- Crystal Reports Server Settings
 - Allow Report Jobs to Stay Connected to the Database until the Report Job is Closed 1059
 - Batch Size 1059
 - Browse Data Size 1059
 - Cache Files Directory 1059
 - Database Records Read When Previewing or Refreshing 1059
 - Idle Connection Timeout 1059
 - Idle Job Timeout 1059
 - Maximum Cache Size 1059

servers (*continued*)Crystal Reports Server Settings (*continued*)

- Maximum Concurrent Jobs 1059
- Maximum Concurrent Report Jobs 1059
- Maximum Lifetime Jobs Per Child 1059
- Maximum Number of Prestarted Children 1059
- Number of database records to read when previewing or refreshing a report 1059
- Oldest On-Demand Data Given to Clients 1059
- Share Report Data Between Clients 1059
- Single Sign-On Expiry 1059
- Temporary Directory 1059
- Viewer Refresh Always Yields Current Data 1059
- Dashboard Analytics Server 78
- Dashboard Server 79
- default settings 150, 187, 532
- default, for scheduling objects 804
- deleting 177
- Desktop Intelligence Cache Server 79
- Desktop Intelligence Job Server 80
- Desktop Intelligence Processing Server 80
- Desktop Intelligence Server Settings
 - Allow Running VBA 1082
 - Cache Files Directory 1082
 - Cache to Keep When Document Cache is Full 1082
 - Enable CORBA Client Support 1082
 - Enable Execution Traces 1082
 - Enable HTTP Client Support 1082
 - Idle Connection Timeout 1082
 - Idle Job Timeout 1082
 - Idle Transient Object Timeout 1082
 - Maximum Cache Size 1082
 - Maximum Concurrent Jobs 1082
 - Maximum Operations Before Re-setting a Report Job 1082

Index

servers (*continued*)

- Desktop Intelligence Server Settings (*continued*)
 - Oldest On-Demand Data Give to Clients 1082
 - Preloaded Report Jobs 1082
 - Share Report Data Between Clients 1082
 - Single Sign-On Expiry 1082
 - Temporary Directory 1082
 - Viewer Refresh Always Yields Current Data 1082
- disabling 172
- enabling 172
- Event Server 81
- File Repository Servers 81
- for viewing and modifying reports 804
- granting service account rights 309, 310
- grouping 178
- host identification options 189
- hostname 191
- in new node 165
- Input File Repository Servers 82
- IPv6 address 191
- Job Servers 83
- list 152
- List of Values (LOV) Job Server 84
- logging activity 542
- metrics, viewing 534
- modifying group membership 181
- Multi-Dimensional Analysis Server 84
- navigation tree 152
- nodes 60
- Output File Repository Servers 82
- Performance Management Server Settings 1093
- performance settings 184, 553
- placeholders 176
- PM Metrics Server 85
- PM Repository Server 85
- PM Rules Server 86
- Predictive Analysis Server 86

servers (*continued*)

- Process Analysis Server 87
- Program Job Server 87
- properties 184, 553
- Publication Job Server 88
- registering by name 197
- Report Application Server 88
- restarting 168
- set IP address 191
- Sets Profile Server 89
- Sets Query Server 89
- setting service account 305
- standard command-line options 647
- starting 168, 171
 - automatically 168
- status 152, 167
- stopping 168
- UNIX signal handling 650
- user account, changing 227
- Voyager Server Settings
 - Log level 1091
 - Maximum Client Sessions 1091
 - Maximum size of the thread pool 1091
 - Service Startup Timeout 1091
- Web Application Container Server 90
- Web Intelligence Server 90
- Web Intelligence Server Settings
 - Allow Document Map Maximum Size Errors 1073
 - Binary Stream Maximum Size 1073
 - Cache Timeout 1073
 - Disable Cache Sharing 1073
 - Document Cache Clean-up Interval 1073
 - Enable Document Cache 1073
 - Enable List of Values Cache 1073
 - Enable Memory Analysis 1073
 - Enable Real-Time Cache 1073
 - Idle Connection Timeout 1073
 - Idle Document Timeout 1073
 - Images Directory 1073
 - List of Values Batch Size 1073
 - Maximum Character Stream Size 1073

servers (*continued*)Web Intelligence Server Settings (*continued*)

- Maximum Connections 1073
- Maximum Custom Sort Size 1073
- Maximum Document Cache Reduction Space 1073
- Maximum Document Cache Size 1073
- Maximum Document in Cache 1073
- Maximum Document per User 1073
- Maximum Documents Before Recycling 1073
- Maximum List of Values Size 1073
- Memory Lower Threshold 1073, 1081
- Memory Maximum Threshold 1073, 1081
- Memory Upper Threshold 1073, 1081
- Output Cache Directory 1073
- Server Polling Interval 1073
- Single Sign-On Expiry 1073
- Timeout Before Recycling 1073
- Universe Cache Maximum Size 1073

Xcelsius Cache Server 91

Xcelsius Server Settings

- Allow Report Jobs to Stay Connected to the Database until the Report Job is Closed 1070
- Browse Data Size 1070
- Cache Files Directory 1070
- Database Records Read When Previewing or Refreshing 1070
- Idle Connection Timeout 1070
- Idle Job Timeout 1070
- Maximum Cache Size 1070
- Maximum Concurrent Jobs 1070
- Maximum Concurrent Report Jobs 1070
- Maximum Lifetime Jobs Per Child 1070
- Maximum Number of Prestarted Children 1070
- Oldest On-Demand Data Given to Clients 1070
- Share Report Data Between Clients 1070

servers (*continued*)Xcelsius Server Settings (*continued*)

- Single Sign-On Expiry 1070
- Temporary Directory 1070
- Viewer Refresh Always Yields Current Data 1070

servers and architecture, Content Search 977

servers configuration settings, importing 247

service account

- configuring servers 311
- constrained delegation 308
- delegation 305
- setting up 305

service account rights 309

- granting 310

service categories 152

services

- Business Process BI Service 61
- categories 61
- Central Management Console Service 62
- Central Management Service 62
- Client Auditing Proxy Service 62
- configuration templates 184
- Connection Service 68
- contrast with servers 60
- Core Services 61
- Crystal Reports 66
- Crystal Reports Cache Service 66
- Crystal Reports Processing Service 66
- Crystal Reports Scheduling Service 67
- Crystal Reports Viewing and Modification Service 67
- Desktop Intelligence 68
- Desktop Intelligence Cache Service 68
- Desktop Intelligence Processing Service 69
- Desktop Intelligence Scheduling Service 69
- Destination Delivery Scheduling Service 63
- Event Service 63
- Input Filestore Service 63
- List of Values Scheduling Service 67
- management 41
- Multi-Dimensional Analysis Service 70

Index

services (*continued*)

- Output Filestore Service 64
- Performance Management 69
- processing 43
- Program Scheduling Service 64
- Publishing Post Processing Service 64
- Publishing Service 65
- Query as a Web Service (QaaWS) Service 65
- Replication Service 65
- Search Service 65
- storage 42
- Voyager 70
- Web Intelligence 71
- Web Intelligence Processing Service 71
- Web Intelligence Scheduling and Publishing Service 72
- web services 39
- Web Services SDK 65
- Xcelsius 72
- Xcelsius Cache Service 72
- Xcelsius Processing Service 73
- session variables 139
 - and authentication 128
 - primary authentication 128
- sessions 139
 - tracking 139
 - viewing active 535
- set search language for Content Search 982
- settings
 - database 806
 - InfoView 779
 - initial security levels 705
 - instance limits on folders 907
 - report refresh 800
 - top-level folder rights 723
 - viewing account activity 147
- setup.sh 686
- shared libraries, as processing extensions 136, 813
- signal handling 650
- silentinstall.sh 683
- single sign-on 105, 132, 274, 361
 - anonymous 132
 - anonymous account 706
 - authentication 135
 - Enterprise 135
 - LDAP 277
 - Windows AD 330
 - configuring IIS clients 354
 - configuring Internet Explorer 354
 - disabling Guest account 706
 - end-to-end 134
 - Kerberos 330, 350
 - Kerberos for .NET InfoView 352
 - NTLM for .NET InfoView 358
 - setting up
 - LDAP 291
 - SiteMinder 291, 361
 - Windows AD 330
 - Windows NT 272
 - to BusinessObjects Enterprise 132
 - to database 133
 - troubleshooting 292
 - Windows NT 274
- SiteMinder 292
 - configuring LDAP plug-in 291
 - error 292
 - setting up single sign-on with LDAP 291, 361
 - troubleshooting 292
 - Windows AD 361, 362
- sites
 - access levels 736
 - managing rights 403
- SMTP destinations, setting defaults 215
- special characters in Content Search 970
- SPN utility 305
- SSL 235
 - certificates 236
 - configuring servers 235
 - configuring Web Application Container Servers (WACS) 483, 486
 - keys 236

- SSL persistence 56
- SSL. See Secure Sockets Layer (SSL) 277
- sslc.cnf 235
- sslc.exe 235
- startservers 682
- statistics, auditing web activity 141
- status, viewing and changing for servers 167
- stemming, in Content Search 970
- sticky session persistence 56
- stop words 970
- stopservers 683
- storage services 42
- Strategy Builder, rights 1034
- styles, setting CMC preferences 702
- subfolders, deleting 904
- subgroups, adding 758
- subscription 952
- suggested queries 975
- synchronizing auditing actions 600
- syslog 542
- system database, migrating 198
- system events, auditable 577
- system information file (ODBC) 222
- system metrics, viewing 541
 - Web Application Container Server (WACS) 502, 503
- system security 126

T

- temporary files
 - configuring Processing Server 212
- terminating the indexing process 991
- text, scheduling format options 869
- third-party groups, replicating 408
- third-party security plug-ins 134
- third-party users, replicating 408
- thumbnails, adding with reports 906, 911
- tickets 138
 - for distributed security 138
 - logon tokens 137
- time zones, setting CMC preferences 702
- tokenization, in Content Search 970
- Tomcat
 - connect port, changing 197
 - JAAS 318
 - Java options 320
 - Kerberos 315
- tools, administration 700
- top-level
 - creating new categories 909
 - creating new folders 904
 - folders, rights 723
- tracing
 - configuring
 - command line 232
- tracking, sessions 139
- transfer of trust 138
- Translation Manager 58
- troubleshooting
 - error messages 437
 - Kerberos 327, 495
 - LDAP accounts 294
 - single sign-on 292
 - Web Application Container Servers (WACS) 501
- troubleshooting network interfaces 194
- trust, active trust relationship 137
- Trusted Authentication 371, 763
 - configuring in web.xml 373
- two-way replication 413
- type-specific rights 717
 - access levels 1008
 - BI Widgets 1036
 - categories 1000
 - CMC 1012
 - Crystal reports 1002
 - dashboards 1008
 - Designer 1035
 - Desktop Intelligence 1015
 - Desktop Intelligence documents 1003
 - folders 1000
 - groups 1006
 - InfoView 1013

Index

- type-specific rights (*continued*)
 - notes 1001
 - Performance Management 1024
 - Strategy Builder 1034
 - universe connections 1012
 - universes 1009
 - users 1006
 - Web Intelligence 1020
 - Web Intelligence documents 1004

U

- uninstall 682
- uninstallCE.sh 682
- universe 103
- Universe Builder 59
- universe connections
 - auditing configuration 598
 - deleting 787
 - managing 787
 - replicating 409
 - rights 1012
- Universe Designer 59
- universe object security 1011
- universes
 - managing 787
 - replicating 409
 - rights 1009
- UNIX
 - and NT authentication 264
 - syslog 542
- unmanaged disk destination 855
 - setting defaults 218
- unmapping, Windows NT accounts 269
- user accounts 748
 - configuring servers 227
 - creating 754
 - default 748
 - deleting 755
 - managing 748, 753
 - modifying 755

- user aliases 769
 - assigning 769
 - creating 768
 - for existing users 768
 - for new users 767
 - deleting 769
 - disabling 770
- user events, auditable 577
- user folders 909
- users
 - assigning advanced rights to 722
 - assigning rights to 722
 - checking rights for 724, 725
 - granting access to 765
 - rights 1006
 - rights, on top-level folders 723
 - viewing active sessions 535
 - viewing rights for 720

V

- variables, for profile values 962
- versions, differences between releases 159
- view time security, Content Search 974
- Viewers Java SDK 95
- viewers, setting CMC preferences 702
- viewing 535
 - active users 535
 - CMS cluster details 541
 - Crystal reports 802
 - current account activity 147
 - current metrics 534
 - licensing information 146
 - rights for principals 720
 - server metrics 534
 - system metrics 541
 - Web Application Container Server (WACS)
 - metrics 502, 503
- views 104
- Vintela 330
- Voyager 52

W

WAR files

- and BusinessObjects Enterprise web applications 510, 511
- modifying web.config 352
- OpenDocument 330

wdeploy 49

Web Application Container Server (WACS)

- AD Kerberos 495
- adding 476
- adding CMC services 481
- changing memory settings 506
- cloning 480
- CMC service 470
- common tasks 473
- connectors 470
- creating new servers 479
- deleting 481
- firewalls 500
- HTTPS 483, 486, 499
- installing 477
- JAAS files 493
- Kerberos configuration files 492
- load balancing 498
- logging 501
- on multihomed machines 500
- overview 470
- properties 508
- removing 476
- removing CMC services from 482
- resolving port conflicts 503, 504, 505
- restoring system defaults 507
- SSL 483, 486
- system metrics 502, 503
- troubleshooting 501
- using with other web servers 497
- using with proxy servers 498, 499

Web Application Container Service (WACS)
101

web application servers 92

- .NET 97

web application servers (*continued*)

- authentication 128

- Java 94

Web Intelligence 53, 659, 780

- application rights 780
- Job Server 659
- Processing Server 666
- Query HTML access rights 780
- rights 1020
- sample auditing reports 599

Web Intelligence documents

- Publishing formats 949
- rights 1004
- selecting cache options 875
- server for scheduling 804
- updating prompts 808
- viewing universes 821

Web Intelligence Job Server

- destinations 213

Web Intelligence Processing Service 71

Web Intelligence Rich Client 60

Web Intelligence Scheduling and Publishing
Service 72

Web Intelligence Server 90

web response speeds, improving 558

web servers

- improving response speeds 558
- securing 140

web services 39, 99

- configuration for reverse proxy servers 521
- custom deployment 423
- file caching 423
- Query as a Web Service 100
- session variable 423

Web Services SDK 65

web.xml 765, 766

- adding CMS clusters 244
- Trusted Authentication 371

WebLogic

- JAAS configuration file 318
- Java options 321
- Kerberos 315

Index

- WebSphere
 - JAAS 319
 - Java options 322
 - Kerberos 317
- what's new 27
- Windows
 - Event Log 542
 - Local System account 219
 - server dependencies 227
- Windows AD
 - accounts and groups
 - group graph 302
 - scheduling updates 302
 - authentication 294
 - enabling Kerberos 313, 490
 - Kerberos configuration
 - application server 304
 - IIS 313
 - Oracle 313
 - Tomcat 312
 - WebLogic 313
 - WebSphere 313
 - mapping accounts 297
 - mapping groups 297
 - mapping LDAP 278
 - NTLM configuration 329
 - security plug-in 296
- Windows NT 274
 - adding accounts to mapped groups 271
 - authentication 264
 - authentication and UNIX 264
- Windows NT (*continued*)
 - creating groups 272
 - disabling accounts 272
 - managing accounts 265
 - mapping accounts 266
 - in CMC 266
 - mapping groups 266
 - security plug-in 264
 - unmapping accounts 269
 - unmapping groups 269
 - viewing
 - users and groups 270
- Windows NT Challenge/Response
 - authentication 140, 330
- Windows NT single sign-on, setting up 272
- Word, scheduling format options 869
- workflows 110
 - access control lists, assigning principals to 722
 - advanced rights, assigning 722
 - profiles and Publishing 957
 - Publishing 934
 - setting top-level folder rights 723
 - viewing rights 720

X

- Xcelsius 60, 544
- Xcelsius Cache Service 72
- Xcelsius Processing Service 73
- XML, scheduling format options 869