



## Information platform services Administrator Guide

- Information platform services 4.0 Feature Pack 3

2012-03-15

## Copyright

© 2011 SAP AG. All rights reserved. SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, 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. Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company. Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary. These materials are subject to change without notice. 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.

2012-03-15

# Contents

<b>Chapter 1</b>	<b>Getting Started.....</b>	<b>13</b>
1.1	About this help.....	13
1.1.1	Who should use this help?.....	13
1.1.2	About Information platform services.....	13
1.1.3	Variables.....	14
1.2	Before you start.....	14
1.2.1	Key concepts.....	15
1.2.2	Key administrative tools.....	15
1.2.3	Key tasks.....	16
<b>Chapter 2</b>	<b>Architecture.....</b>	<b>19</b>
2.1	Architecture overview.....	19
2.1.1	System overview.....	19
2.1.2	Databases.....	20
2.1.3	Servers.....	21
2.1.4	Web application servers.....	22
2.1.5	Language support.....	23
2.1.6	Authentication and single sign-on.....	24
2.1.7	SAP integration.....	26
2.1.8	Lifecycle management (LCM).....	27
2.1.9	Integrated version control.....	27
2.1.10	Upgrade path.....	27
2.2	Conceptual tiers.....	28
2.3	Services and servers.....	29
2.3.1	Services.....	31
2.3.2	Service categories.....	33
2.3.3	Server types.....	34
2.3.4	Server categories.....	35
2.4	Client applications.....	37
2.4.1	Central Configuration Manager (CCM).....	37
2.4.2	Upgrade management tool.....	37
2.4.3	Web application clients.....	38

2.5	Process Workflows.....	39
2.5.1	Startup and authentication.....	39
2.5.2	Program objects.....	41
<b>Chapter 3</b>	<b>Managing Licenses.....</b>	<b>43</b>
3.1	Managing License keys.....	43
3.1.1	To view license information.....	43
3.1.2	To add a license key.....	43
3.1.3	To view current account activity.....	44
3.2	Measuring licenses.....	44
3.2.1	To run a license audit.....	45
<b>Chapter 4</b>	<b>Managing Users and Groups.....</b>	<b>47</b>
4.1	Account management overview.....	47
4.1.1	User management.....	47
4.1.2	Group management.....	49
4.1.3	Available authentication types .....	50
4.2	Managing Enterprise and general accounts.....	52
4.2.1	To create a user account.....	52
4.2.2	To modify a user account.....	53
4.2.3	To delete a user account.....	54
4.2.4	To create a new group.....	54
4.2.5	To modify a group's properties.....	55
4.2.6	To view group members.....	55
4.2.7	To add subgroups.....	55
4.2.8	To specify group membership.....	56
4.2.9	To delete a group.....	56
4.2.10	To enable the Guest account.....	57
4.2.11	Adding users to groups.....	57
4.2.12	Changing password settings.....	59
4.2.13	Granting access to users and groups.....	60
4.2.14	Controlling access to user inboxes.....	61
4.2.15	Configuring BI launch pad options.....	61
4.3	Managing aliases.....	65
4.3.1	To create a user and add a third-party alias.....	65
4.3.2	To create a new alias for an existing user.....	66
4.3.3	To assign an alias from another user.....	66
4.3.4	To delete an alias.....	67
4.3.5	To disable an alias.....	67

<b>Chapter 5</b>	<b>Setting Rights.....</b>	<b>69</b>
5.1	How rights work in Information platform services.....	69
5.1.1	Access levels.....	69
5.1.2	Advanced rights settings.....	70
5.1.3	Inheritance.....	71
5.1.4	Type-specific rights.....	76
5.1.5	Determining effective rights.....	77
5.2	Managing security settings for objects in the CMC.....	78
5.2.1	To view rights for a principal on an object.....	79
5.2.2	To assign principals to an access control list for an object.....	79
5.2.3	To modify security for a principal on an object.....	80
5.2.4	To set rights on a top-level folder in Information platform services.....	80
5.2.5	Checking security settings for a principal.....	81
5.3	Working with access levels.....	83
5.3.1	Choosing between View and View On Demand access levels.....	85
5.3.2	To copy an existing access level.....	86
5.3.3	To create a new access level.....	87
5.3.4	To rename an access level.....	87
5.3.5	To delete an access level.....	87
5.3.6	To modify rights in an access level.....	88
5.3.7	Tracing the relationship between access levels and objects.....	89
5.3.8	Managing access levels across sites.....	89
5.4	Breaking inheritance.....	90
5.4.1	To disable inheritance.....	91
5.5	Using rights to delegate administration.....	92
5.5.1	Choosing between Modify the rights users have to objects options.....	93
5.5.2	Owner rights.....	95
5.6	Summary of recommendations for rights administration.....	95
<b>Chapter 6</b>	<b>Securing Information platform services.....</b>	<b>97</b>
6.1	Security overview .....	97
6.2	Disaster recovery planning.....	97
6.3	General recommendations for securing your deployment.....	98
6.4	Configuring security for bundled third-party servers.....	99
6.5	Active trust relationship.....	99
6.5.1	Logon tokens.....	99
6.5.2	Ticket mechanism for distributed security.....	100
6.6	Sessions and session tracking.....	100
6.6.1	CMS session tracking.....	101

6.7	Environment protection.....	101
6.7.1	Web browser to web server.....	102
6.7.2	Web server to Information platform services.....	102
6.8	Auditing security configuration modifications.....	102
6.9	Auditing web activity.....	103
6.9.1	Protection against malicious logon attempts.....	103
6.9.2	Password restrictions.....	103
6.9.3	Logon restrictions.....	104
6.9.4	User restrictions.....	104
6.9.5	Guest account restrictions.....	104
6.10	Processing extensions.....	105
6.11	Overview of Information platform services data security.....	105
6.11.1	Data processing security modes.....	106
6.12	Cryptography in Information platform services.....	108
6.12.1	Working with cluster keys.....	108
6.12.2	Cryptographic Officers.....	111
6.12.3	Managing cryptographic keys in the CMC.....	112
6.13	Configuring servers for SSL.....	116
6.13.1	Creating key and certificate files.....	117
6.13.2	Configuring the SSL protocol.....	119
6.14	Understanding communication between Information platform services components.....	123
6.14.1	Overview of Information platform services servers and communication ports.....	123
6.14.2	Communication between Information platform services components .....	126
6.15	Configuring BI platform for firewalls.....	133
6.15.1	To configure the system for firewalls.....	133
6.15.2	Debugging a firewalled deployment.....	136
6.16	Examples of typical firewall scenarios.....	138
6.16.1	Example - Application tier deployed on a separate network.....	138
6.16.2	Example - Thick client and database tier separated from Information platform services servers by a firewall.....	140
6.17	Firewall settings for integrated ERP environments.....	143
6.17.1	Specific firewall guidelines for SAP integration.....	143
6.17.2	Firewall configuration for JD Edwards EnterpriseOne integration.....	145
6.17.3	Specific firewall guidelines for Oracle EBS.....	147
6.17.4	Firewall configuration for PeopleSoft Enterprise integration .....	148
6.17.5	Firewall configuration for Siebel integration.....	150
6.18	Information platform services and reverse proxy servers .....	151
6.18.1	Supported reverse proxy servers .....	152
6.18.2	Understanding how web applications are deployed .....	152
6.19	Configuring reverse proxy servers for Information platform services web applications.....	152
6.19.1	Detailed instructions for configuring reverse proxy servers.....	153

6.19.2	To configure the reverse proxy server.....	153
6.19.3	To configure Apache 2.2 reverse proxy server for Information platform services .....	154
6.19.4	To configure WebSEAL 6.0 reverse proxy server for Information platform services .....	154
6.19.5	To configure Microsoft ISA 2006 for Information platform services .....	155
6.20	Special configuration for Information platform services in reverse proxy deployments.....	157
6.20.1	Enabling reverse proxy for Information platform services Web Services.....	157
6.20.2	Enabling the root path for session cookies for ISA 2006.....	158
6.20.3	Enabling reverse proxy for SAP BusinessObjects Live Office.....	159
<b>Chapter 7</b>	<b>Authentication.....</b>	<b>161</b>
7.1	Authentication options in Information platform services .....	161
7.1.1	Primary authentication.....	162
7.1.2	Security plug-ins.....	163
7.1.3	Single sign-on to Information platform services.....	164
7.2	Enterprise authentication.....	166
7.2.1	Enterprise authentication overview.....	166
7.2.2	Enterprise authentication settings.....	166
7.2.3	To change Enterprise settings.....	167
7.2.4	Enabling Trusted Authentication.....	169
7.2.5	Configuring Trusted Authentication for the web application.....	170
7.3	LDAP authentication.....	179
7.3.1	Using LDAP authentication.....	179
7.3.2	Configuring LDAP authentication.....	181
7.3.3	Mapping LDAP groups.....	192
7.4	Windows AD authentication.....	196
7.4.1	Overview.....	196
7.4.2	Preparing for AD authentication (Kerberos).....	200
7.4.3	AD authentication single sign-on.....	210
7.4.4	Mapping AD groups and configuring AD authentication.....	220
7.4.5	Troubleshooting Windows AD authentication.....	225
7.5	SAP authentication.....	227
7.5.1	Configuring SAP authentication .....	227
7.5.2	Creating a user account for Information platform services.....	228
7.5.3	Connecting to SAP entitlement systems.....	229
7.5.4	Setting SAP Authentication options.....	231
7.5.5	Importing SAP roles.....	236
7.5.6	Setting up single sign-on to the SAP system.....	239
7.6	PeopleSoft authentication.....	243
7.6.1	Overview.....	243
7.6.2	Enabling PeopleSoft Enterprise authentication.....	243
7.6.3	Mapping PeopleSoft roles to Information platform services.....	244

7.6.4	Scheduling user updates.....	247
7.6.5	Using the PeopleSoft Security Bridge.....	249
7.7	JD Edwards authentication.....	260
7.7.1	Overview.....	260
7.7.2	Enabling JD Edwards EnterpriseOne authentication.....	260
7.7.3	Mapping JD Edwards EnterpriseOne roles to Information platform services.....	261
7.7.4	Scheduling user updates.....	264
7.8	Siebel authentication.....	266
7.8.1	Enabling Siebel authentication.....	266
7.8.2	Mapping roles to Information platform services.....	267
7.8.3	Scheduling user updates.....	270
7.9	Oracle EBS authentication.....	272
7.9.1	Enabling Oracle EBS authentication.....	272
7.9.2	Mapping Oracle E-Business Suite roles to Information platform services.....	273
7.9.3	Unmapping roles .....	278
7.9.4	Customizing rights for mapped Oracle EBS groups and users .....	279
7.10	Automated user updates.....	280
7.10.1	Scheduling user updates.....	280
<b>Chapter 8</b>	<b>Server Administration.....</b>	<b>283</b>
8.1	Server Administration.....	283
8.1.1	Working with the Servers management area in the CMC.....	283
8.1.2	Managing servers by using scripts on Windows .....	287
8.1.3	Managing servers on Unix.....	287
8.1.4	Managing License keys.....	287
8.1.5	Measuring licenses.....	289
8.1.6	Viewing and changing a server's status.....	290
8.1.7	Adding, cloning, or deleting servers.....	295
8.1.8	Clustering Central Management Servers.....	298
8.1.9	Managing server groups.....	302
8.1.10	Assessing your system's performance.....	306
8.1.11	Configuring server settings.....	308
8.1.12	Configuring server network settings.....	312
8.1.13	Managing Nodes.....	320
8.1.14	Renaming a computer in an Information platform services deployment.....	341
8.1.15	Managing server and node placeholders.....	341
<b>Chapter 9</b>	<b>Managing Web Application Container Servers (WACS).....</b>	<b>343</b>
9.1	WACS.....	343
9.1.1	Web Application Container Server (WACS).....	343

9.1.2	Adding or removing additional WACS to your deployment.....	346
9.1.3	Adding or removing services to WACS.....	350
9.1.4	Configuring HTTPS/SSL.....	351
9.1.5	Supported authentication methods.....	355
9.1.6	Configuring AD Kerberos for WACS .....	356
9.1.7	Configuring AD Kerberos single sign-on .....	362
9.1.8	WACS and your IT environment.....	364
9.1.9	Troubleshooting.....	366
9.1.10	WACS properties.....	370
<b>Chapter 10</b>	<b>Backing up and Restoring.....</b>	<b>373</b>
10.1	Hot backups.....	373
10.2	Enabling hot backups.....	373
10.2.1	To enable hot backups.....	374
<b>Chapter 11</b>	<b>Copying your system.....</b>	<b>375</b>
11.1	Overview of system copying.....	375
11.2	Terminology.....	375
11.3	Use cases.....	375
11.4	Planning to copy your system.....	377
11.5	Considerations and limitations.....	378
11.6	System copy procedure.....	380
11.6.1	To perform a system copy export from a source system.....	380
11.6.2	To perform a system copy import to a target system.....	383
<b>Chapter 12</b>	<b>Lifecycle Management.....</b>	<b>385</b>
12.1	About promotion management.....	385
12.2	Version Management System settings for Lifecycle Management Console.....	385
12.2.1	Version Management System Supported Options .....	391
12.2.2	Configuring ClearCase on BI Platform.....	391
12.2.3	Creating and Configuring SubVersion Repository Manually.....	392
12.3	BIAR Engine Command-Line Tool.....	393
12.3.1	Using a properties file .....	396
12.3.2	To use the BIAR Engine Command-Line Tool.....	400
<b>Chapter 13</b>	<b>Monitoring.....</b>	<b>403</b>
13.1	About Monitoring.....	403
13.2	Monitoring terms.....	403
13.2.1	Architecture.....	404
13.3	Cluster support for monitoring server.....	407

13.4	Metrics.....	408
13.5	Configuration properties.....	412
13.5.1	JMX end point URL.....	415
13.6	Integrating with other applications.....	416
13.6.1	Integrating the monitoring application with IBM Tivoli.....	417
13.6.2	Integrating the monitoring application with SAP Solution Manager .....	420
13.7	Creating Universe for Derby Database.....	420
13.8	Troubleshooting.....	421
13.8.1	Dashboard.....	421
13.8.2	Alerts.....	422
13.8.3	Watchlist.....	422
13.8.4	Probes.....	423
13.8.5	Metrics.....	423
13.8.6	Graph.....	424
<b>Chapter 14</b>	<b>Auditing.....</b>	<b>425</b>
14.1	Overview.....	425
14.2	CMC Auditing page.....	431
14.2.1	Auditing Status Summary.....	431
14.2.2	Configuring Auditing events.....	433
14.2.3	Auditing Data Store configuration settings.....	435
14.3	Audit events.....	436
14.3.1	Audit events and details.....	445
<b>Chapter 15</b>	<b>Supportability.....</b>	<b>461</b>
15.1	Logging traces from components.....	461
15.2	Trace log levels.....	461
15.3	Configuring tracing for servers.....	462
15.3.1	To set the server trace log level in the CMC.....	463
15.3.2	To set the trace log level for multiple servers managed in the CMC.....	463
15.3.3	To configure server tracing through the BO_trace.ini file.....	464
15.4	Configuring tracing for web applications.....	467
15.4.1	To set the web application trace log level in the CMC.....	467
15.4.2	To manually modify tracing settings through the BO_trace.ini file.....	468
15.5	Configuring tracing for Upgrade management tool.....	473
15.5.1	To configure tracing for Upgrade management tool.....	473
<b>Chapter 16</b>	<b>Command line administration.....</b>	<b>475</b>
16.1	Command lines overview.....	475
16.1.1	To view or modify a server's command line.....	475

16.2	Standard options for all servers.....	475
16.2.1	UNIX signal handling.....	476
16.3	Central Management Server.....	476
16.4	Job servers.....	478
16.5	Adaptive Processing Server.....	479
16.6	Input and Output File Repository Servers.....	479
<b>Chapter 17</b>	<b>Rights appendix.....</b>	<b>481</b>
17.1	About the rights appendix.....	481
17.2	General rights.....	481
17.3	Rights for specific object types.....	484
17.3.1	Folder rights.....	484
17.3.2	Categories.....	484
17.3.3	Notes.....	485
17.3.4	Users and groups.....	485
17.3.5	Access levels.....	486
17.3.6	Applications.....	487
<b>Chapter 18</b>	<b>Server properties appendix.....</b>	<b>489</b>
18.1	About the server properties appendix.....	489
18.1.1	Common server properties.....	489
18.1.2	Core Services properties.....	492
<b>Chapter 19</b>	<b>Server metrics.....</b>	<b>505</b>
19.1	About the Server Metrics Appendix.....	505
19.1.1	Common Server Metrics .....	505
19.1.2	Central Management Server metrics.....	508
19.1.3	File Repository Server Metrics.....	512
19.1.4	Adaptive Processing Server metrics.....	513
19.1.5	Web Application Container Server metrics.....	519
19.1.6	Adaptive Job Server metrics.....	520
<b>Chapter 20</b>	<b>Nodes and placeholders.....</b>	<b>523</b>
20.1	Server and node placeholders.....	523
<b>Chapter 21</b>	<b>Auditing Database Schema Appendix.....</b>	<b>537</b>
21.1	Overview.....	537
21.2	Schema diagram.....	537
21.3	Auditing Data Store Tables.....	538

<b>Appendix A</b>	<b>More Information.....</b>	<b>549</b>
<b>Index</b>		<b>551</b>

# Getting Started

## 1.1 About this help

This help provides you with information and procedures for deploying and configuring your Information platform services 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 *Information platform services Administrator's Guide*.

For information about installing this product, see the *Information platform services Installation Guide*.

### 1.1.1 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 an Information platform services 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.

### 1.1.2 About Information platform services

Information platform services 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, Information platform services delivers tangible benefits that extend across and beyond the organization. As an integrated suite for reporting, analysis, and information delivery, Information platform services provides a solution for increasing end-user productivity and reducing administrative efforts.

### 1.1.3 Variables

The following variables are used throughout this guide.

Variable	Description
<INSTALLDIR>	The directory where Information platform services is installed. On a Windows computer, the default directory is C:\Program Files (x86)\SAP BusinessObjects\.
<PLATFORM64DIR>	The name of your Unix operating system. Acceptable values are: <ul style="list-style-type: none"> <li>• aix_rs6000_64</li> <li>• linux_x64</li> <li>• solaris_sparcv9</li> <li>• hpux_ia64</li> </ul>
<SCRIPTDIR>	The directory where scripts for administering Information platform services are located. On a Windows computer, the directory is <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts. On a Unix computer, the directory is <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64DIR>/scripts.

### 1.2 Before you start

## 1.2.1 Key concepts

SAP BusinessObjects Business Intelligence (BI) platform uses the terms “service” and “server” to refer to the two types of software running on a BI platform computer.

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

A *server* is a process at the operating system level (on some systems, called a *daemon*) that hosts one or more services. For example, the Central Management Server (CMS) and Adaptive Processing Server are servers. A server runs on a specific operating system account and has its own PID.

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

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

## 1.2.2 Key administrative tools

### 1.2.2.1 Central Management Console (CMC)

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

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

### 1.2.2.2 Central Configuration Manager (CCM)

The Central Configuration Manager (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 command line.

You use the CCM to create and configure nodes and to start or stop your web application server, if it is the default bundled Tomcat web application server. On Windows, it also allows you to configure network parameters, such as Secure 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 is now used for troubleshooting and node configuration.

### 1.2.2.3 Upgrade management tool

Upgrade management tool (formerly Import Wizard) is installed as a part of Information platform services, and guides administrators through the process of importing users, groups, and folders from previous versions of Information platform services. It also allows you to import and upgrade objects, events, server groups, repository objects, and calendars.

For information on upgrading from a previous version of Information platform services, see the *Information platform services Upgrade Guide*.

## 1.2.3 Key tasks

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.

**Related Topics**

- [Planning or performing your first deployment](#)
- [Configuring your deployment](#)
- [Improving your system's performance](#)
- [Central Management Console \(CMC\)](#)

### 1.2.3.1 Planning or performing your first deployment

If you are planning or performing your first deployment of Information platform services, perform the following tasks and read the recommended topics:

- “Architecture overview”
- “Communication between Information platform services components”
- “Security overview”
- “Authentication options in Information platform services”, if you plan to use third-party authentication
- After installation, “Server Administration”

For more information about installing this product, see the *Information Platform Services Installation Guide*.

#### Related Topics

- [Architecture overview](#)
- [Communication between Information platform services components](#)
- [Security overview](#)
- [Authentication options in Information platform services](#)
- [Server Administration](#)

### 1.2.3.2 Configuring your deployment

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

#### Related Topics

- [Server Administration](#)
- [Security overview](#)
- [About Monitoring](#)

### 1.2.3.3 Improving your system's performance

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

- “About Monitoring” if you want to monitor your existing system
- “Server Administration” for daily maintenance tasks and procedures for working with servers in the CMC

#### Related Topics

- [About Monitoring](#)
- [Server Administration](#)

### 1.2.3.4 Working with objects in the CMC

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

- For information about setting up users and groups in the CMC, see “Account Management Overview”.
- To set security on objects, see “How rights work in Information platform services”.
- For general information about working with objects, see the *Information platform services CMC Help*.

#### Related Topics

- [Account management overview](#)
- [How rights work in Information platform services](#)

# Architecture

## 2.1 Architecture overview

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

Information platform services 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 by creating dedicated servers to host specific services. The architecture is designed to meet the needs of virtually any BI deployment, and is flexible enough to grow from several users with a single tool, to tens of thousands of users with multiple tools and interfaces.

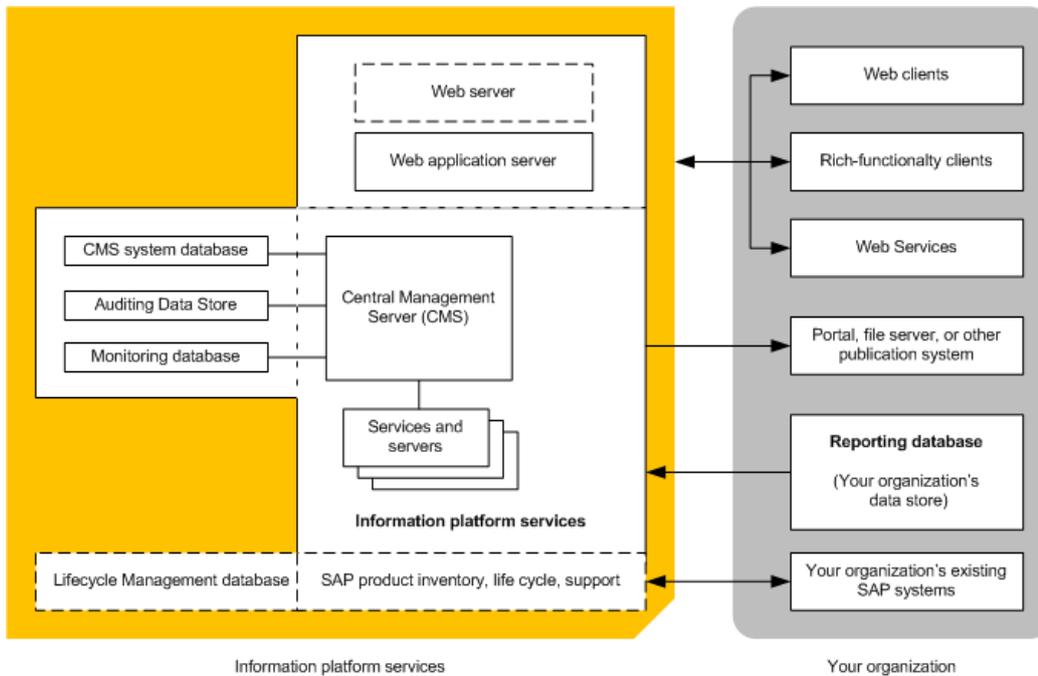
To provide flexibility, reliability, and scalability, Information platform services components can be installed on one or across many machines. You can even install two different versions of Information platform services simultaneously on the same computer, although this configuration is only recommended as part of the upgrade process 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 multiple, redundant, versions of the same server process on more than one machine, so that processing can continue if the primary process encounters a problem.

### 2.1.1 System overview

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

The following diagram illustrates how Information platform services fits in with your organization's infrastructure.



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

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

## 2.1.2 Databases

Information platform services uses several different databases.

- Reporting database

This refers to your organization's information. It is the source information analyzed and reported on by Information platform services. Most commonly, the information is stored within a relational database, but it can also be contained within text files, Microsoft Office documents, or OLAP systems.

- CMS system database

The CMS system database is used to store Information platform services information, such as user, server, folder, document, configuration, authorization, and authentication details. It is maintained by the Central Management Server (CMS), and is sometimes referred to as the *system repository*.

- Auditing Data Store

The Auditing Data Store (ADS) is used to store information on trackable events that occur in Information platform services. This information can be used to monitor the usage of system components, user activity, or other aspects of day-to-day operation.

- Lifecycle Management database

The Lifecycle Management database tracks configuration and version information related to an Information platform services installation, as well as updates.

- Monitoring database

Monitoring uses the Java Derby database to store system configuration and component information for SAP supportability.

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

## 2.1.3 Servers

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

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

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

The advantages of having multiple servers include:

- Improved performance

Multiple Information platform services server hosts can process a queue of reporting information faster than a single Information platform services server host.

- Load balancing

If a server is experiencing a higher load than the other servers in a cluster, the CMS automatically sends new work to a server with better resources.

- Improved availability

If a server encounters an unexpected condition, the CMS automatically re-routes work to different servers until the condition is corrected.

## 2.1.4 Web application servers

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

The following web application servers are supported:

- JBoss
- Oracle Application Server
- SAP NetWeaver AS Java
- Tomcat
- WebLogic
- WebSphere

For a detailed list of supported web application servers, consult the *Supported Platforms Guide* available at: <http://service.sap.com/bosap-support>.

If you do not have a web application server in place for use with Information platform services, the installation program can install and configure a Tomcat 6 web application server for you. It is recommended that you evaluate your requirements against information from your web application server vendor to determine which supported web application server would best suit your organization's requirements.

**Note:**

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

### 2.1.4.1 Web Application Container Service (WACS)

A web application server is required to host Information platform services web applications.

If you are an advanced Java web application server administrator with advanced administration needs, use a supported Java web application server to host Information platform services web applications. If you will be using a supported Windows operating system to host Information platform services, and prefer a simple web application server installation process, or you do not have the resources to administer a Java web application server, you can install the Web Application Container Service (WACS) when installing Information platform services.

WACS is an Information platform services server that allows Information platform services web applications, such as the Central Management Console (CMC) and Web Services, to run without the need for a previously installed Java web application server.

Using WACS to provides a number of advantages:

- WACS requires a minimum effort to install, maintain, and configure. It is installed and configured by the Information platform services installation program, and no additional steps are required to start using it.
- WACS removes the need for Java application server administration and maintenance skills.
- WACS provides an administrative interface that is consistent with other Information platform services servers.
- Like other Information platform services servers, WACS can be installed on a dedicated host.

**Note:**

There are some limitations to using WACS instead of a dedicated Java web applications server:

- WACS is only available on supported Windows operating systems.
- Custom web applications cannot be deployed to WACS, as it only supports the web applications installed with Information platform services.
- WACS cannot be used with an Apache load balancer.

It is possible to use a dedicated web application server in addition to WACS. This allows your dedicated web application server to host custom web applications, while the CMC and other Information platform services web applications are hosted by WACS.

## 2.1.5 Language support

Information platform services products are translated into many different languages and supports data in an even broader selection of languages.

Product interfaces are available in the following languages:

- Czech
- Simplified Chinese
- Traditional Chinese
- Danish
- Dutch
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Norwegian Bokmal
- Polish
- Portuguese
- Russian

- Spanish
- Swedish
- Thai

In addition to supporting data in any of the languages available in the interface, the following character sets are also supported:

- Greek
- Malaysian
- Hebrew
- Arabic
- Romanian
- Vietnamese
- Hungarian
- Turkish
- Hindi

## **2.1.6 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 Information platform services, its folders, and other objects.

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

- Enterprise (default), including Trusted Authentication support for third-party authentication.
- LDAP
- Windows Active Directory (AD)

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

- SAP ERP and Business Warehouse (BW)
- Oracle E-Business Suite (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

### **2.1.6.1 Security plug-ins**

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

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

Information platform services supports the following security plug-ins:

- Enterprise security plug-in

The Central Management Server (CMS) handles security information, such as user accounts, group memberships, and object rights that define user and group privileges. This is known as Enterprise authentication.

Enterprise authentication is always enabled; it cannot be disabled. Use the system default Enterprise Authentication if you prefer to create distinct accounts and groups for use with Information platform services, or if you have not already set up a hierarchy of users and groups on an LDAP or Windows AD server.

Trusted Authentication is a component of Enterprise authentication that integrates with third-party single sign-on solutions, including Java Authentication and Authorization Service (JAAS). Applications that have established trust with the Central Management Server can use Trusted Authentication to allow users to log on without providing their passwords.

- LDAP security plug-in
- Windows AD

**Note:**

Although a user can configure Windows AD authentication for Information platform services and custom applications through the CMC, the CMC does not support Windows AD authentication with NTLM. The only methods of authentication that the CMC support are Windows AD with Kerberos, LDAP, Enterprise, and Trusted Authentication.

### **2.1.6.2 Enterprise Resource Planning (ERP) integration**

An Enterprise Resource Planning (ERP) application supports the essential functions of an organization's processes by collecting real-time information related to day-to-day operations. SAP BusinessObjects Business Intelligence platform supports single sign-on and reporting from a number of ERP systems. See the *SAP BusinessObjects BI 4.0 Product Availability Matrix (PAM)*, available at <http://service.sap.com/pam>.

SAP ERP and BW support is installed by default. Use the Custom / Expand installation option to deselect SAP integration support if you do not want support for SAP ERP or BW. Support for other ERP systems

is not installed by default. Use the "Custom / Expand" installation option to select and install integration for non-SAP ERP systems.

To configure ERP integration, see the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

## 2.1.7 SAP integration

Information platform services integrates with your existing SAP infrastructure with the following SAP tools:

- SAP System Landscape Directory (SLD)

The system landscape directory of SAP NetWeaver is the central source of system landscape information relevant for the management of your software life-cycle. By providing a directory comprising information about all installable software available from SAP and automatically updated data about systems already installed in a landscape, you get the foundation for tool support to plan software life-cycle tasks in your system landscape.

The Information platform services installation program registers the vendor and product names and versions with the SLD, as well as server and front-end component names, versions, and location.

- SAP Solution Manager

The SAP Solution Manager is a platform that provides the integrated content, tools, and methodologies to implement, support, operate and monitor an organization's SAP and non-SAP solutions.

Non-SAP software with an SAP-certified integration is entered into a central repository and transferred automatically to your SAP System Landscape Directories (SLD). SAP customers can then easily identify which version of third-party product integration has been certified by SAP within their SAP system environment. This service provides additional awareness for third-party products besides our online catalogs for third-party products.

SAP Solution Manager is available to SAP customers at no extra charge, and includes direct access to SAP support and SAP product upgrade path information. For more information on SLD, see "Registration of Information platform services in the System Landscape" in the *Information platform services Administrator Guide*.

- CTS Transport (CTS+)

The Change and Transport System (CTS) helps you to organize development projects in ABAP Workbench and in Customizing, and then transport the changes between the SAP systems in your system landscape. As well as ABAP objects, you can also transport Java objects (J2EE, JEE) and SAP-specific non-ABAP technologies (such as Web Dynpro Java or SAP NetWeaver Portal) in your landscape.

- Monitoring with CA Wily Introscope

CA Wily Introscope is a web application management product that delivers the ability to monitor and diagnose performance problems that may occur within Java-based SAP modules in production,

including visibility into custom Java applications and connections to back-end systems. It allows you to isolate performance bottlenecks in NetWeaver modules including individual Servlets, JSPs, EJBs, JCO's, Classes, Methods and more. It offers real-time, low-overhead monitoring, end-to-end transaction visibility, historical data for analysis or capacity planning, customizable dashboards, automated threshold alarms, and an open architecture to extend monitoring beyond NetWeaver environments.

## 2.1.8 Lifecycle management (LCM)

Lifecycle management (LCM) refers to a set of processes involved in managing an installation's product information. It establishes procedures for governing the installation of Information platform services to development, test, production, or maintenance environments.

Information platform services Lifecycle Manager is a web-based tool that enables you to move BI objects from one system to another system, without affecting the dependencies of those objects. It also enables you to manage different versions, manage dependencies, or roll back a promoted object to its previous state.

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

For more information, see the *Information platform services Lifecycle management console User's Guide*.

## 2.1.9 Integrated version control

The files that make up SAP BusinessObjects Business Intelligence platform on a server system are now kept under version control. The installation program will install and configure the Subversion version control system, or you can enter details to use an existing Subversion or ClearCase version control system.

A version control system makes it possible to keep and restore different revisions of configuration and other files, which means it is always possible to revert the system to a known state from any time in the past.

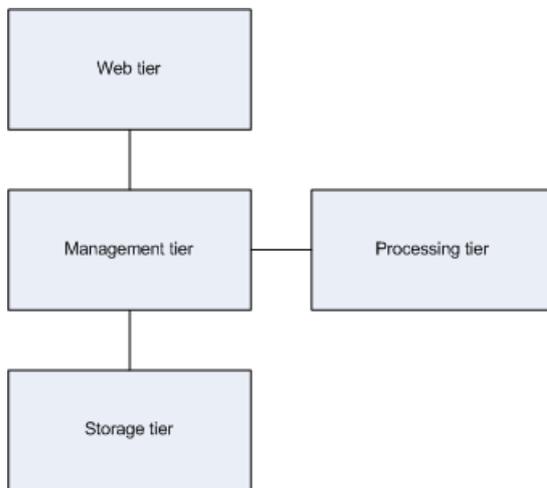
## 2.1.10 Upgrade path

It's possible to upgrade from a previous release of Information platform services, but you must first install Information platform services 4.0, then migrate the settings and data from your existing system with the Upgrade management tool.

For information on how to upgrade from a previous version, see the *Information platform services Upgrade Guide*.

## 2.2 Conceptual tiers

Information platform services can be thought of as a series of conceptual tiers:



- Web tier

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

The web tier also contains Web Services. Web Services provides Information platform services functionality to software tools via the web application server, such session authentication, user privilege management, scheduling, search, administration, reporting, and query management.

- Management tier

The management tier coordinates and controls all of the components that make up Information platform services. It is comprised of the Central Management Server (CMS). The CMS provides maintains security and configuration information, sends service requests to servers, manages auditing, and maintains the CMS system database.

- Processing tier

The processing tier analyzes data and produces reports. This is the only tier that accesses the databases that contain report data.

- Storage tier

The storage tier is responsible to handling files, such as documents and reports. The Input File Repository Server manages files that contain information to be used in reports. The Output File Repository Server manages reports created by the system. The storage tier also handles report caching to save system resources when users access reports.

## 2.3 Services and servers

Information platform services uses the terms “server” and “service” to refer to the two types of software running on an Information platform services computer.

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 Interactive Analysis Scheduling and Publishing Service is a subsystem that runs on the Adaptive Job Server.

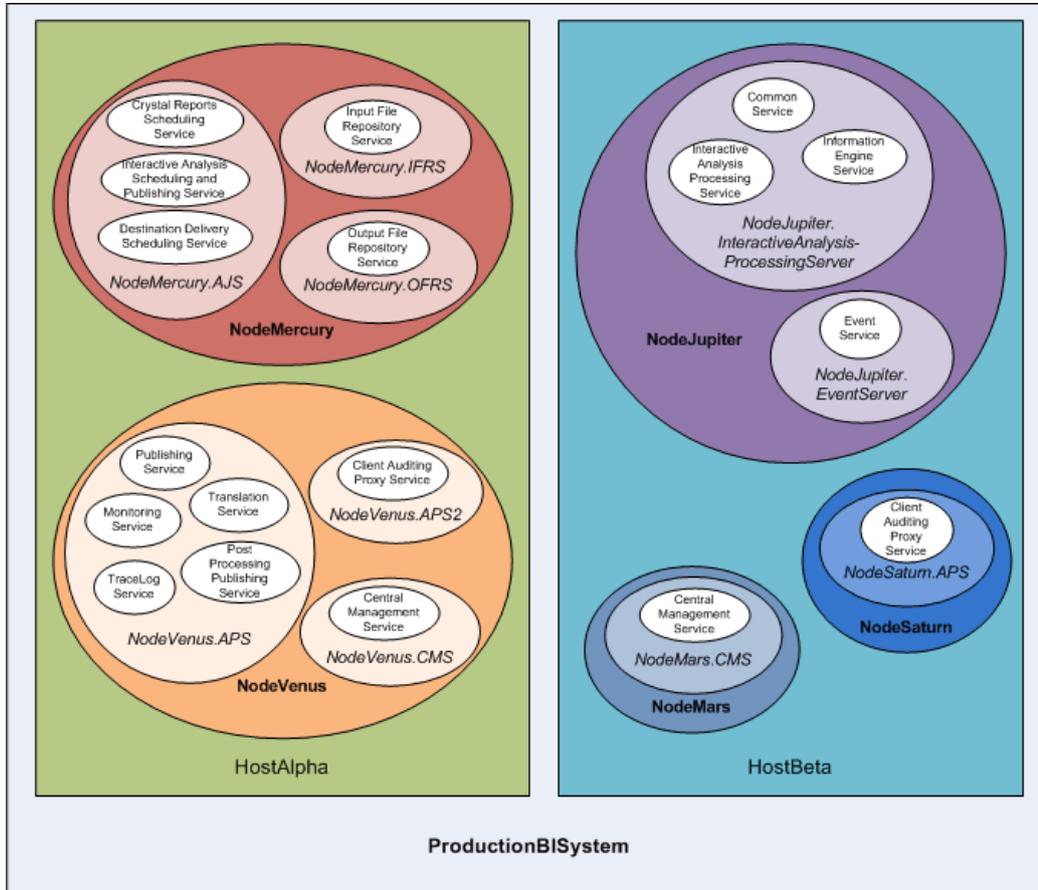
A server is used to describe an operating system level process (on some systems, this is referred to as a daemon) hosting one or more services. For example, the Central Management Server (CMS) and Adaptive Processing Server are servers. A server runs under a specific operating system account and has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

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

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

### **Services, servers, nodes, and hosts**

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



Two hosts form the cluster named ProductionBISystem, which has two hosts:

- The host named HostAlpha has Information platform services installed and is configured with two nodes:
  - NodeMercury contains an Adaptive Job Server (NodeMercury.AJS) with services to schedule and publish reports, an Input File Repository Server (NodeMercury.IFRS) with a service to store input reports, and an Output File Repository Server (NodeMercury.OFRS) with a service to store report output.
  - NodeVenus contains an Adaptive Processing Server (NodeVenus.APS) with services to provide publishing, monitoring, and translation features, an Adaptive Processing Server (NodeVenus.APS2) with a service to provide client auditing, and a Central Management Server (NodeVenus.CMS) with a service to provide the CMS services.
- The host named HostBeta has Information platform services installed and is configured with three nodes:
  - NodeMars contains a Central Management Server (NodeMars.CMS) with a service to provide the CMS services.

Having the CMS on two computers enables load balancing and mitigation and failover capabilities.

- NodeJupiter contains a Interactive Analysis Processing Server (`NodeJupiter.InteractiveAnalysis`) with a service to provide Interactive Analysis reporting, and an Event Server (`NodeJupiter.EventServer`) to provide report monitoring of files.
- NodeSaturn contains an Adaptive Processing Server (`NodeSaturn.APS`) with a service to provide client auditing.

### Related Topics

- [Server Administration](#)

## 2.3.1 Services

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

### Note:

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

Service	Service category	Server type	Service description
Authentication Update Scheduling Service	Core Services	Adaptive Job Server	Provides synchronization of updates for third-party security plugins
Central Management Service	Core Services	Central Management Server	Provides server, user, session management, and security (authorization and authentication) management. At least one Central Management Service must be available in a cluster for the cluster to operate.
Destination Delivery Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled jobs and publishes the results to a given output location, such as the file system, FTP, email, or a user's inbox

<b>Service</b>	<b>Service category</b>	<b>Server type</b>	<b>Service description</b>
Input Filestore Service	Core Services	Input File Repository Server	Maintains published report and program objects that can be used in the generation of new reports when an input file is received
Lifecycle Management ClearCase Service	Lifecycle Management Services	Adaptive Processing Server	Provides ClearCase support for LCM
Lifecycle Management Scheduling Service	Lifecycle Management Services	Adaptive Job Server	Runs scheduled Lifecycle Management jobs
Lifecycle Management Service	Lifecycle Management Services	Adaptive Processing Server	Lifecycle Management Core service
Monitoring Service	Core Services	Adaptive Processing Server	Provides monitoring functions
Multi Dimensional Analysis Service	Advanced Analysis Services	Adaptive Processing Server	Provides access to multi-dimensional Online Analytical Processing (OLAP) data; converts the raw data into XML, which can be rendered into Excel, PDF, or Advanced Analysis (formerly Voyager) crosstabs and charts
Output Filestore Service	Core Services	Output File Repository Server	Maintains collection of completed documents
Probe Scheduling Service	Core Services	Adaptive Job Server	Provides scheduled Probe jobs and publishes the results to a given output location
Program Scheduling Service	Core Services	Adaptive Job Server	Runs programs that have been scheduled to run at a given time
RESTful Web Service	Core Services	Web Application Container Server (WACS)	Provides session handling for RESTful Web Service requests.
Security Query Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled Security Query jobs

Service	Service category	Server type	Service description
Security Token Service	Core Services	Adaptive Processing Server	SAP Single Sign-On support
Web Services SDK and QaaWS	Core Services	Web Application Container Server	Web Services on WACS

### Related Topics

- [Service categories](#)
- [Server types](#)

## 2.3.2 Service categories

### Note:

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

Service category	Service	Server type
Advanced Analysis Services	Multi Dimensional Analysis Service	Adaptive Processing Server
Core Services	Authentication Update Scheduling Service	Adaptive Job Server
Core Services	Central Management Service	Central Management Server
Core Services	Client Auditing Proxy Service	Adaptive Processing Server
Core Services	Destination Delivery Scheduling Service	Adaptive Job Server
Core Services	Input Filestore Service	Input File Repository Server
Core Services	Monitoring Service	Adaptive Processing Server
Core Services	Output Filestore Service	Output File Repository Server
Core Services	Probe Scheduling Service	Adaptive Job Server
Core Services	Program Scheduling Service	Adaptive Job Server
Core Services	RESTful Web Service	Web Application Container Server (WACS)

Service category	Service	Server type
Core Services	Security Query Scheduling Service	Adaptive Job Server
Core Services	Security Token Service	Adaptive Processing Server
Lifecycle Management Services	LifeCycle Management ClearCase Service	Adaptive Processing Server
Lifecycle Management Services	Lifecycle Management Scheduling Service	Adaptive Job Server
Lifecycle Management Services	Lifecycle Management Service	Adaptive Processing Server

### Related Topics

- [Services](#)
- [Server types](#)

## 2.3.3 Server types

### Note:

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

Server type	Service	Service category
Adaptive Job Server	Authentication Update Scheduling Service	Core Services
Adaptive Job Server	Destination Delivery Scheduling Service	Core Services
Adaptive Job Server	Lifecycle Management Scheduling Service	Lifecycle Management Services
Adaptive Job Server	Probe Scheduling Service	Core Services
Adaptive Job Server	Program Scheduling Service	Core Services
Adaptive Job Server	Security Query Scheduling Service	Core Services
Adaptive Processing Server	Client Auditing Proxy Service	Core Services

Server type	Service	Service category
Adaptive Processing Server	Lifecycle Management ClearCase Service	Lifecycle Management Services
Adaptive Processing Server	Lifecycle Management Service	Lifecycle Management Services
Adaptive Processing Server	Monitoring Service	Core Services
Adaptive Processing Server	Multi Dimensional Analysis Service	Advanced Analysis Services
Adaptive Processing Server	Security Token Service	Core Services
Central Management Server	Central Management Service	Core Services
Dashboard Analytics Server	Dashboard Analytics Service	Core Services
Input File Repository Server	Input Filestore Service	Core Services
Output File Repository Server	Output Filestore Service	Core Services
Web Application Container Server (WACS)	RESTful Web Service	Core Services

#### Related Topics

- [Services](#)
- [Service categories](#)

### 2.3.4 Server categories

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

Server categories	Description
Adaptive Job Server	<p>General server that processes scheduled jobs. When you add a Job server to the Information platform services system, you can configure the Job server to process reports, documents, programs, or publications and send the results to different destinations.</p>
Adaptive Processing Server	<p>A generic server that hosts services responsible for processing requests from a variety of sources.</p> <p><b>Note:</b> The installation program installs one Adaptive Processing Server (APS) per host system. Depending on the features that you've installed, this APS may host a large number of services, such as the Monitoring Service, Lifecycle Management Service, Multi-Dimensional Analysis Service (MDAS), Publishing Service, and others.</p> <p>If you are installing a production environment, do not use the default APS. Instead, it is highly recommended that once the installation process is complete, you perform a system sizing to determine:</p> <ul style="list-style-type: none"> <li>• The type and number of APS services.</li> <li>• The distribution of services across multiple APS servers.</li> <li>• The optimal number of APS servers. Multiple APS servers provide redundancy, better performance, and higher reliability.</li> <li>• The distribution of APS servers across multiple nodes.</li> </ul> <p>Create new APS server instances as determined by the sizing process.</p> <p>For example, if the outcome of your sizing happens to suggest the creation of one APS for each service category, then may end up creating eight APS servers. One for each service category: Advanced Analysis Services, Connectivity Services, Core Services, Crystal Reports Services, Dashboards Services, Data Federation Services, Lifecycle Management Services, and Interactive Analysis Services.</p>
Central Management Server (CMS)	<p>Maintains a database of information about your Information platform services system (in the CMS system database) and audited user actions (in the Auditing Data Store). All platform services are managed by the CMS. The CMS also controls access to the system files where documents are stored, and information on users, user groups, security levels (including authentication and authorization), and content.</p>
File Repository Server	<p>Responsible for the creation of file system objects, such as exported reports, and imported files in non-native formats. An Input FRS stores report and program objects that have been published to the system by administrators or end users. An Output FRS stores all of the report instances generated by the Job Server.</p>

## 2.4 Client applications

You can interact with Information platform services using two different types of desktop applications:

- Desktop applications

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

Desktop clients allow you to offload some BI report processing onto individual client computers. Most desktop applications directly access your organization's data through drivers installed on the desktop, and communicate with your Information platform services deployment through CORBA or encrypted CORBA SSL.

- Web applications

These applications are hosted by a web application server and can be accessed with a supported web browser on Windows, Macintosh, Unix, and Linux operating systems.

This allows you to provide business intelligence (BI) access to large groups of users, without the challenges of deploying desktop software products. Communication is conducted over HTTP, with or without SSL encryption (HTTPS).

### 2.4.1 Central Configuration Manager (CCM)

The Central Configuration Manager (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 command line.

You use the CCM to create and configure nodes and to start or stop your web application server, if it is the default bundled Tomcat web application server. On Windows, it also allows you to configure network parameters, such as Secure 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 is now used for troubleshooting and node configuration.

### 2.4.2 Upgrade management tool

Upgrade management tool (formerly Import Wizard) is installed as a part of Information platform services, and guides administrators through the process of importing users, groups, and folders from previous

versions of Information platform services. It also allows you to import and upgrade objects, events, server groups, repository objects, and calendars.

For information on upgrading from a previous version of Information platform services, see the *Information platform services Upgrade Guide*.

### **2.4.3 Web application clients**

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

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

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

1. Standalone mode

All web application resources are deployed to a web application server that serves both dynamic and static content. This arrangement is suitable for small installations.

2. Split mode

The web application's static content (HTML, images, CSS) is deployed to a dedicated web server, while dynamic content (JSPs) is deployed to a web application server. This arrangement is suitable for larger installations that will benefit from the web application server being freed up from serving static web content.

For more information about WDeploy, see the *Information platform services Web Application Deployment Guide*.

#### **2.4.3.1 Central Management Console (CMC)**

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

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

## 2.5 Process Workflows

When tasks are performed such as logging in or scheduling an object, 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 Information platform services system.

### 2.5.1 Startup and authentication

#### 2.5.1.1 Logging on to Information platform services

This workflow describes a user logging on to a Information platform services web application such as the Central Management Console (CMC) from a web browser.

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

#### 2.5.1.2 SIA start-up

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

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

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

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

**Note:**

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

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

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

### **2.5.1.3 SIA shutdown**

You can automatically stop the Server Intelligence Agent (SIA) by shutting down the host operating system, or you can manually stop the SIA in the Central Configuration Manager (CCM).

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

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

**Note:**

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

## 2.5.2 Program objects

### 2.5.2.1 A scheduled program object runs

This workflow describes the process of a scheduled program object running at a scheduled time.

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

**Note:**

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

4. The Program Scheduling Service launches the program.
5. The Program Scheduling Service updates the CMS periodically with the job status. The current status is Processing.
6. The Program Scheduling Service sends a log file to the Output FRS. The Output FRS notifies the Program Scheduling Service that the object was scheduled successfully by sending an object log file.

**Note:**

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

7. The Program Scheduling Service updates the CMS with the job status. The current status is Success.
8. The CMS updates the job status in its memory and then writes the instance information to the CMS system database.

### 2.5.2.2 Setting a schedule for a program object

This workflow describes the process of a user scheduling a program object to be run at a future time from a web application such as the Central Management Console (CMC).

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

# Managing Licenses

## 3.1 Managing License keys

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

### Related Topics

- [To add a license key](#)
- [To view license information](#)
- [To view current account activity](#)

### 3.1.1 To view license information

The **License Keys** management area of the CMC identifies the number of role-based (BI Viewer and BI Analyst), concurrent, named, and processor licenses that are associated with each key.

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

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

### Related Topics

- [Managing License keys](#)
- [To add a license key](#)
- [To view license information](#)

### 3.1.2 To add a license key

If you are upgrading from a trial version of the product, be sure to delete the Evaluation key prior to adding any new license keys or product activation keycodes.

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

The key is added to the list.

#### **Related Topics**

- [To add a license key](#)
- [To view current account activity](#)

### **3.1.3 To view current account activity**

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

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

#### **Related Topics**

- [Managing License keys](#)
- [To add a license key](#)
- [To view license information](#)

## **3.2 Measuring licenses**

The BusinessObjects License Measurement Tool (BOLMT) is a java command-line utility used to collect and store Information platform services licensing data. The output XML document contains license deployment measurements and is sent to SAP Global License Auditing Services (GLAS) for consolidation as part of a license audit.

The system administrator installs and runs BOLMT for every Information platform services cluster whenever a license audit is requested. BOLMT collects usage measurements on role-based, named, and concurrent user licenses.

The administrator can specify a particular output directory for the XML document, and configure the output document to not contain any information that may be used to identify system users.

### 3.2.1 To run a license audit

To perform a license audit, you will need administrator rights and access to the directory containing the `BOLMT.jar` file in the Information platform services installation.

1. Open a command line console.
2. Change directories to the directory containing the java executables for your Information platform services installation

By default the file is installed in the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib` directory.

3. Execute the `BOLMT.jar`.

The execution command is entered in the following format: `-jar BOLMT.jar [options] <outputFile>`

The table below summarizes the available options:

Option	Description
<code>-c --cms</code>	Specifies the name identifier and port number for the Central Management Server (CMS). Specified as <code>cmsname:port number</code> . By default, the CMS settings for the local host are used if this setting is not specified.
<code>-p --password</code>	Specifies the administrator account password used to connect to the CMS.
<code>-a--auth</code>	Specifies the authentication method to connect user to the CMS. Default method is Enterprise specified as <code>secEnterprise</code> .
<code>-s--sanitize</code>	Specifies that the output audit document should filter out any personal information that may be used to identify users.

**Note:**

The output file specification is always the last argument in the command line. It is an optional setting. If no argument is specified, the output goes to the console's standard output. You can also pipe output to script as a command line argument.

**Example:**

```
C:\Program Files (x86)\SAP
Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\lib>"C:\Program Files
(x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
\java.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```



# Managing Users and Groups

## 4.1 Account management overview

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

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

### 4.1.1 User management

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

Table 4-1: Default user accounts

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

### 4.1.1.1 Role-based licensing

Under the user-role based licensing scheme, there are two roles which can be assigned to Information platform services users:

- BI Analyst
- BI Viewer

Each role is bundled with specific access levels to Information platform services applications. You cannot modify or override the access level to either user role. User roles apply to new user accounts created in Information platform services or existing users imported from third party directory services such as Windows AD or LDAP.

**Note:**

User roles should not be confused with group membership. When you assign a user one of the two available roles, the user is automatically assigned predefined rights to applications. To associate a user with specific group access levels, you must add the user to the desired group.

Click **License Key** in the CMC for more information on your licensing scheme, or contact your SAP Business Objects account manager for further information on access rights for each user role.

#### 4.1.1.1.1 BI Analyst role

The BI Analyst role is designed for users who create content in the Information platform services system. Users who edit or create reports, design and manage universes, or perform any administrative tasks in the CMC should be assigned the BI Analyst role.

#### 4.1.1.1.2 BI Viewer role

The BI Viewer role is designed primarily for content consumers. These users only view reports but do not modify content.

Users assigned to the BI Viewer role will be prevented by the system from creating content, modifying reports and performing general administrative tasks in the system. The BI Viewer role should not be assigned to users who need to:

- Create reports
- Update or modify reports
- Perform administrative tasks using the CMC

**Note:**

BI Viewer users cannot access the CMC.

## 4.1.2 Group management

Groups are collections of users who share the same account privileges; therefore, you may create groups that are based on department, role, or location. Groups enable you to change the rights for users in one place (a group) instead of modifying the rights for each user account individually. Also, you can assign object rights to a group or groups.

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

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

Table 4-2: Default group accounts

Account name	Description
<b>Administrators</b>	Members of this group can perform all tasks in all of the Information platform services applications (CMC, CCM, Publishing Wizard, and BI launch pad). By default, the <b>Administrators</b> group contains only the Administrator user.
<b>Everyone</b>	Each user is a member of the <b>Everyone</b> group.
<b>QaaWS Group Designer</b>	Members of this group have access to Query as a Web Service.
<b>Report Conversion Tool Users</b>	Members of this group have access to the Report Conversion Tool application.
<b>Translators</b>	Members of this group have access to the Translation Manager application.

Account name	Description
<p><b>Universe Designer Users</b></p>	<p>Users who belong to this group are granted access to the <b>Universe Designer</b> folder and the <b>Connections</b> 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.</p>

**Related Topics**

- [How rights work in Information platform services](#)
- [Granting access to users and groups](#)

**4.1.3 Available authentication types**

Before setting up user accounts and groups within Information platform services, 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 4-3: Authentication types*

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

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

## 4.2 Managing Enterprise and general accounts

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

### Note:

When a user logs off their web session on Information platform services by navigating to a non-Information platform services 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 Information platform services.

### 4.2.1 To create a user account

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

1. Go to the "Users and Groups" management area of the CMC.
2. Click **Manage > New > New User**.  
The "New User" dialog box appears.
3. To create an Enterprise user,
  - a. Select **Enterprise** from the **Authentication Type** list.
  - b. Type the account name, full name, email, and description information.

### Tip:

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

- c. Specify the password information and settings.
4. To create a user that will logon using a different authentication type, select the appropriate option from the **Authentication Type** list, and type the account name.
  5. Specify how to designate the user account according to options stipulated by your Information platform services license agreement.

If your license agreement is based on user roles, select one of the following options:

- **BI Viewer:** access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.
- **BI Analyst:** access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all applications workflows

that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications

If your license agreement is not based on user roles, specify a connection type for the user account.

- 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 Information platform services regardless of the number of other people who are currently connected.

6. Click **Create & Close**.

The user is added to the system and is automatically added to the Everyone group. An inbox is automatically created for the user, together with an Enterprise alias. You can now add the user to a group or specify rights for the user.

#### **Related Topics**

- [How rights work in Information platform services](#)
- [Role-based licensing](#)

## **4.2.2 To modify a user account**

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

#### **Note:**

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

1. Go to the "Users and Groups" management area of the CMC.
2. Select the user whose properties you want to change.
3. Click **Manage > Properties**.

The "Properties" dialog box for the user appears.

4. Modify the properties for the user.

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

#### **Note:**

Any changes you make to the user account do not appear until the next time the user logs on.

5. Click **Save & Close**.

#### **Related Topics**

- [To create a new alias for an existing user](#)

### 4.2.3 To delete a user account

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

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

**Note:**

Deleting a user account won't necessarily prevent the user from being able to log on to Information platform services 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 Information platform services, 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 disable an alias](#)

### 4.2.4 To create a new group

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

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

## 4.2.5 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**.

## 4.2.6 To view group members

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

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

**Note:**

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

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

## 4.2.7 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](#)

## 4.2.8 To specify group membership

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

1. In the "Users and Groups" management area of the CMC, click the group that you want to add to another group.
2. Click **Actions > Member Of**.  
The "Member Of" dialog box appears.
3. Click **Join Group**.  
The "Join Group" dialog box appears.
4. Move the group that you want to add the first group to from the **Available Groups** to the **Destination Group(s)** list.  
Any rights associated with the parent group will be inherited by the new group you have created.
5. Click **OK**.  
You return to the "Member Of" dialog box, and the parent group appears in the parent groups list.

## 4.2.9 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 SAP BusinessObjects Windows AD Users group, use the "Authentication" management area in CMC.

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

#### 4.2.10 To enable the Guest account

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

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

1. Go to the "Users and Groups" management area of the CMC.
2. Click **User List** 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**.

#### 4.2.11 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](#)

#### 4.2.11.1 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 Information platform services 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**.

#### 4.2.11.2 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**.

## 4.2.12 Changing password settings

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

### 4.2.12.1 To change user password settings

1. Go to the "Users and Groups" management area of the CMC.
2. Select the user whose password settings you want to change.
3. Click **Manage > Properties**.  
The "Properties" dialog box appears.
4. Select or clear the check box associated with the password setting you want to change.  
The available options are:
  - **Password never expires**
  - **User must change password at next logon**
  - **User cannot change password**
5. Click **Save & Close**.

### 4.2.12.2 To change general password settings

1. Go to the "Authentication" management area of the CMC.
2. Double-click **Enterprise**.  
The "Enterprise" dialog box appears.
3. Select the check box for each password setting that you want to use, and provide a value if necessary.  
The following table identifies the minimum and maximum values for each of the settings you can configure.

Table 4-4: Password settings

<b>Password setting</b>	<b>Minimum</b>	<b>Recommended Maximum</b>
<b>Enforce mixed-case passwords</b>	N/A	N/A
<b>Must contain at least N Characters</b>	0 characters	64 characters
<b>Must change password every N day(s)</b>	1 day	100 days
<b>Cannot reuse the N most recent password(s)</b>	1 password	100 passwords
<b>Must wait N minute(s) to change password</b>	0 minutes	100 minutes
<b>Disable account after N failed attempts to log on</b>	1 failed	100 failed
<b>Reset failed logon count after N minute(s)</b>	1 minute	100 minutes
<b>Re-enable account after N minute(s)</b>	0 minutes	100 minutes

4. Click **Update**.

### 4.2.13 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](#)

## 4.2.14 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**

- [Setting a schedule for a program object](#)
- [Managing security settings for objects in the CMC](#)

## 4.2.15 Configuring BI launch pad options

Administrators can configure the way users access the BI launch pad applications. By configuring properties in the BOE.war file, you can specify what information is available on the user's logon screen. You can also use the CMC to set BI launch pad preferences for specific groups.

### 4.2.15.1 Configuring the BI launch pad logon screen

By default, the BI launch pad 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 BI launch pad properties for the BOE.war file.

#### 4.2.15.1.1 To configure the BI launch pad logon screen

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

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

```
<INSTALLDIR>\Information platform services __MINI-BOE-VERSION__\warfiles\we  
bapps\BOE\WEB-INF\config\custom\
```

**Note:**

If you are using the Tomcat version installed with Information platform services, you can also access the following directory: C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom

- If you are using any other supported web application server, consult the documentation for your web application server to determine the appropriate path.

2. Create a new file.

**Note:**

Use Notepad or any other text-editing utility.

3. Save the file under the following name:

BIlaunchpad.properties

4. To include the authentication options on the BI launch pad logon screen add the following:

```
authentication.visible=true
```

5. To change the default authentication type add the following:

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

Replace <authentication> with any of the following options

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

6. To prompt users for the CMS name on the BI launch pad logon screen :

```
cms.visible=true
```

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

Use WDeploy to redeploy the BOE.war file on the web application server. For more information on using WDeploy, see the *Information Platform Services Web Application Deployment Guide*.

### 4.2.15.2 Configuring BI launch pad Preferences for groups

Administrators can set BI launch pad preferences for specific user groups. These preferences serve as default BI launch pad preferences for all users in the group.

**Note:**

If users have set their own preferences, any administrator-defined settings will not be reflected in their view of BI launch pad. Users can always switch from their own preferences to the administrator-defined preferences at any time and use the updated settings.

By default no BI launch pad preferences are set for any user groups. Administrators can specify preferences for the following:

- Home tab
- Documents - start location
- Folders
- Categories
- Number of objects per page
- Columns displayed in the "Document" tab
- How to display documents in BI launch pad - through tabs or a new window

**4.2.15.2.1 To set BI launch pad Preferences for a group**

1. Go to the "Users and Groups" management area of the CMC.
2. Select the group from the Group List.
3. Click **Actions > BI launch pad Preferences**  
The "BI launch pad Preferences" dialog box appears
4. Unselect **No Preferences Defined**.
5. To set a user's initial view:
  - To display the Home tab when the user first log on, click **Home tab** and choose one of the following options:

Option	Description
<b>Default Home tab</b>	Displays the default Home tab provided with Information platform services will be used.
<b>Select Home tab</b>	Displays a specific website as the home tab.  Click <b>Browse Home tab</b> . In the "Select a Custom Home tab" window, select a repository object and click <b>Open</b> .  <b>Note:</b> you can only select an object that has already been added to the repository.

- To display the Documents tab when the user first log on, click **Documents**, and then specify which drawer and node are open by default. You can select from the following

Drawer	Node options
My Documents	Choose from one of the following to display in the Documents tab: <ul style="list-style-type: none"> <li>• My Favorites</li> <li>• Personal Categories</li> <li>• My Inbox</li> </ul>
Folders	Choose from one of the following: <ul style="list-style-type: none"> <li>• Public Folders: this will display the public folders in the Documents tab</li> <li>• Select Public folder</li> </ul> Click <b>Browse Folder</b> to select a specific public folder to display in the Documents tab.
Categories	Choose from one of the following: <ul style="list-style-type: none"> <li>• Corporate Categories: this will display the corporate categories in the Documents tab</li> <li>• Select Corporate Category</li> </ul> Click <b>Browse Folder</b> to select a specific corporate category to display in the Documents tab.

For example, if you want the **My Documents** drawer to be open to the user's BI Inbox when they first log on, click **My Documents** and click **My Inbox**.

6. Under "Choose columns displayed in Documents tab", select the summary information that you want to see for each object in the user's List panel:
  - **Type**
  - **Last Run**
  - **Instances**
  - **Description**
  - **Created By**
  - **Created On**
  - **Location (Categories)**
  - **Received On (Inbox)**
  - **From (Inbox)**
7. Under "Set document viewing location", choose how you want users to view their documents. Users can open documents for viewing in new tabs within BI launch pad or in new web browser windows.
8. Enter a number in the **Set the maximum number of items per page** field to specify the maximum number of objects displayed per page when a user views lists of objects.
9. Click **Save & Close**.

The specified preferences will serve as defaults for users in the group you selected in Step 2. Users will however be able to create their own BI launch pad preferences, if they have the right to set their

preferences. If you do not want users to modify the preferences, you should not grant users the right to set preferences.

## 4.3 Managing aliases

If a user has multiple accounts in Information platform services, 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 Information platform services, LDAP or Windows AD aliases.

### 4.3.1 To create a user and add a third-party alias

When you create a user and select an authentication type other than Enterprise, the system creates the new user in Information platform services 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 Information platform services.

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

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

### 4.3.2 To create a new alias for an existing user

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

**Note:**

For the system to create the third-party alias, the following criteria must be met:

- The authentication tool needs to have been enabled in the CMC.
- The format of the account name must agree with the format required for the authentication type.
- The user account must exist in the third-party authentication tool, and it must belong to a group that is mapped to Information platform services.

1. Go to the "Users and Groups" management area of the CMC.
2. Select the user that you want to add an alias to.
3. Click **Manage > Properties**.

The "Properties" dialog box appears.

4. Click **New Alias**.
5. Select the authentication type.
6. Type in the account name for the user.
7. Click **Update**.

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

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

### 4.3.3 To assign an alias from another user

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

**Note:**

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

1. Go to the "Users and Groups" management area of the CMC.
2. Select the user you want to assign an alias to.
3. Click **Manage > Properties**.

The "Properties" dialog box appears.

4. Click **Assign Alias**.
5. Enter the user account that has the alias you want to assign, and click **Find Now**.
6. Move the alias you want to assign from the **Available aliases** list to the **Aliases to be added to *Username*** list.

Here *Username* represents the name of the user you are assigning an alias to.

**Tip:**

To select multiple aliases, use the **SHIFT + click** or **CTRL + click** combination.

7. Click **OK**.

### 4.3.4 To delete an alias

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

**Note:**

Deleting a user's alias does not necessarily prevent the user from being able to log on to Information platform services again. If the user account still exists in the third-party system, and if the account belongs to a group that is mapped to Information platform services, then Information platform services 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.

### 4.3.5 To disable an alias

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

**Note:**

Deleting a user from the system does not necessarily prevent the user from being able to log on to Information platform services again. If the user account still exists in the third-party system, and if the account belongs to a group that is mapped to Information platform services, then the system will still allow the user to log on. To ensure a user can no longer use one of his or her aliases to log on to Information platform services, 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](#)

# Setting Rights

## 5.1 How rights work in Information platform services

Rights are the base units for controlling user access to the objects, users, applications, servers, and other features in Information platform services. 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 Information platform services 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 Information platform services 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.

### 5.1.1 Access levels

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

Information platform services 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 Information platform services 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](#)

## 5.1.2 Advanced rights settings

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

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

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

Table 5-1: Rights options

Icon	Rights option	Description
	<b>Granted</b>	The right is granted to a principal.
	<b>Denied</b>	The right is denied to a principal.
	<b>Not Specified</b>	The right is unspecified for a principal. By default, rights set to <b>Not Specified</b> are denied.

Icon	Rights option	Description
	<b>Apply to Object</b>	The right applies to the object. This option becomes available when you click <b>Granted</b> or <b>Denied</b> .
	<b>Apply to Sub Object</b>	The right applies to sub-objects. This option becomes available when you click <b>Granted</b> or <b>Denied</b> .

### Related Topics

- [Type-specific rights](#)

## 5.1.3 Inheritance

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

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

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

Information platform services recognizes two types of inheritance: group inheritance and folder inheritance.

### 5.1.3.1 Group inheritance

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

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

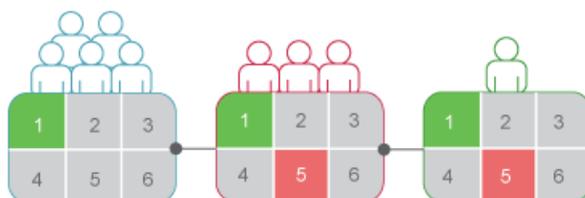


Figure 5-1: Group inheritance example 1

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.

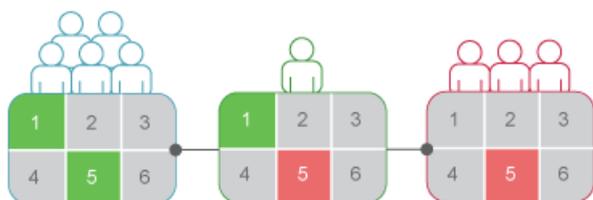


Figure 5-2: Group inheritance example 2

## Related Topics

- [Rights override](#)

### 5.1.3.2 Folder inheritance

Folder inheritance allows principals to inherit any rights that they have been granted on an object's parent folder. Folder inheritance proves especially useful when you organize Information platform services 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.

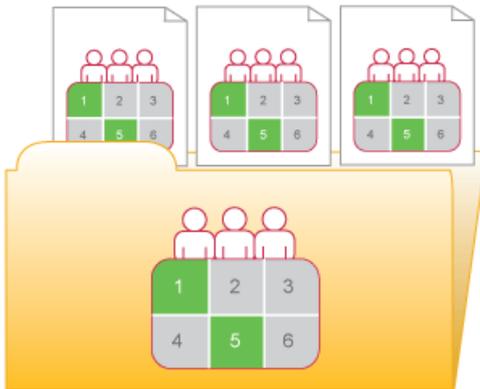


Figure 5-3: Folder inheritance example

#### Related Topics

- [Rights override](#)

### 5.1.3.3 Rights override

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

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

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

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

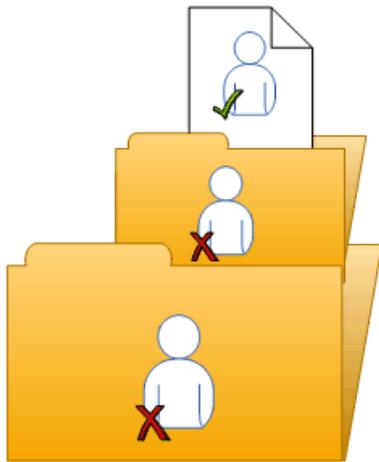


Figure 5-4: Rights override example 1

“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.

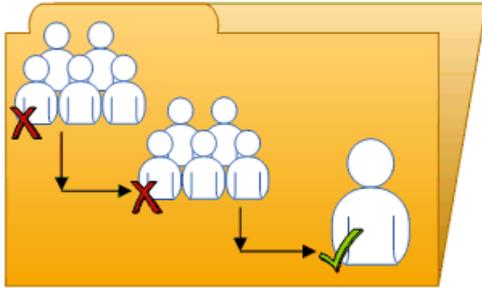


Figure 5-5: Rights override example 2

“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 Information platform services.

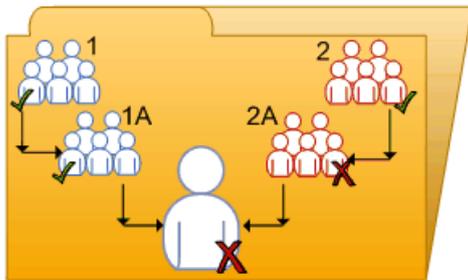


Figure 5-6: Complex rights override

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.

### 5.1.3.4 Scope of rights

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

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

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

### 5.1.4 Type-specific rights

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

- General rights for the object type

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

- Specific rights for the object type

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

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

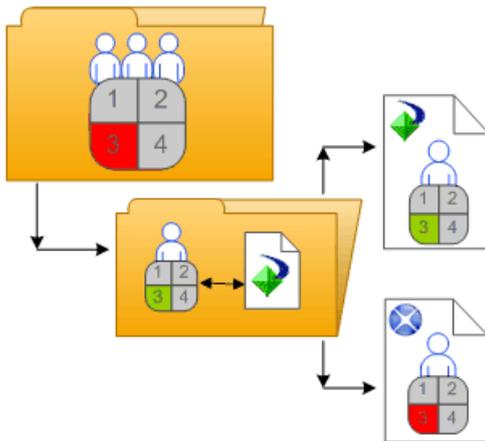


Figure 5-7: Type-specific rights example

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, and Adobe Acrobat PDFs.

- **Application**

These rights are divided according to which Information platform services application they affect. Examples of applications include the CMC and BI launch pad.

- **System**

These rights are divided according to which core system component they affect. Examples of core system components include Calendars, Events, and Users and Groups.

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

## 5.1.5 Determining effective rights

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

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

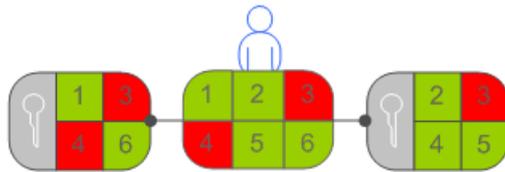


Figure 5-8: Multiple access levels

- 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.

## 5.2 Managing security settings for objects in the CMC

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

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

- Viewing rights for a principal on an object.

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

### 5.2.1 To view rights for a principal on an object

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

1. Select the object for which you want to view security settings.
2. Click **Manage > User Security**.

The "User Security" dialog box appears and displays the access control list for the object.

3. Select a principal from the access control list, and click **View Security**

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

- Browse for another principal whose rights you want to view.
- Filter the rights displayed according to these criteria:
  - assigned rights
  - granted rights
  - unassigned rights
  - from access level
  - object type
  - the name of the right
- Sort the list of rights displayed in ascending or descending order according to these criteria:
  - collection
  - type
  - right name
  - right status (granted, denied, or unspecified)

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

### 5.2.2 To assign principals to an access control list for an object

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

1. Select the object to which you want to add a principal.
2. Click **Manage > User Security**.

The "User Security" dialog box appears and displays the access control list.

3. Click **Add Principals**.

The "Add Principals" dialog box appears.

4. Move the users and groups you want to add as principals from the **Available users/groups** list to the **Selected users/groups** list.

5. Click **Add and Assign Security**.

6. Select the access levels you want to grant the principal.

7. Choose whether to enable or disable folder or group inheritance.

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

#### **Related Topics**

- [To modify security for a principal on an object](#)

### **5.2.3 To modify security for a principal on an object**

In general, it is recommended that you use access levels to assign rights to a principal. However, you may need to override certain granular rights in an access level sometimes. Advanced rights let you customize the rights for a principal on top of the access levels the principal already has. In general, you follow this workflow to assign advanced rights to a principal on an object.

1. Assign the principal to the access control list for the object.

2. When the principal has been added, go to **Manage > User Security** to display the access control list for the object.

3. Select the principal from the access control list, and click **Assign Security**.

The "Assign Security" dialog box appears.

4. Click the **Advanced** tab.

5. Click **Add/Remove rights**.

6. Modify the rights for the principal.

All the available rights are summarized in the *Rights Appendix*.

#### **Related Topics**

- [To assign principals to an access control list for an object](#)

### **5.2.4 To set rights on a top-level folder in Information platform services**

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

**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](#)

## 5.2.5 Checking security settings for a principal

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

- Query principal

You specify the user or group that you want to run the security query for. You can specify one principal for each security query.

- Query permission

You specify the right or rights you want to run the security query for, the status of these rights, and the object type these rights are set on. For example, you can run a security query for all reports that a principal can refresh, or for all reports that a principal cannot export.

- Query context

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

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

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

### 5.2.5.1 To run a security query

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

**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, Information platform services 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.

## 5.3 Working with access levels

You can do the following with access levels:

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

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

Table 5-2: Predefined access levels

Access level	Description	Rights involved
<b>View</b>	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"> <li>• View objects</li> <li>• View document instances</li> </ul>
<b>Schedule</b>	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.	<b>View</b> access level rights, plus: <ul style="list-style-type: none"> <li>• Schedule the document to run</li> <li>• Define server groups to process jobs</li> <li>• Copy objects to another folder</li> <li>• Schedule to destinations</li> <li>• Print the report's data</li> <li>• Export the report's data</li> <li>• Edit objects that the user owns</li> <li>• Delete instances that the user owns</li> <li>• Pause and resume document instances that the user owns</li> </ul>
<b>View On Demand</b>	A principal can refresh data on demand against a data source.	<b>Schedule</b> access level rights, plus: <ul style="list-style-type: none"> <li>• Refresh the report's data</li> </ul>

Access level	Description	Rights involved
<b>Full Control</b>	A principal has full administrative control of the object.	All available rights, including: <ul style="list-style-type: none"> <li>• Add objects to the folder</li> <li>• Edit objects</li> <li>• Modify rights users have to objects</li> <li>• Delete objects</li> <li>• Delete instances</li> </ul>

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"> <li>• <b>Add</b> right on the <b>Access Levels</b> top-level folder</li> </ul>
View granular rights in an access level	<ul style="list-style-type: none"> <li>• <b>View</b> right on the access level</li> </ul>
Assign an access level to a principal on an object	<ul style="list-style-type: none"> <li>• <b>View</b> right on the access level</li> <li>• <b>Use the Access Level for Security Assignment</b> right on the access level</li> <li>• <b>Modify Rights</b> right on the object, or <b>Securely Modify Rights</b> right on the object and the principal</li> </ul> <p><b>Note:</b> Users who have the <b>Securely Modify Rights</b> 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"> <li>• <b>View</b> and <b>Edit</b> rights on the access level</li> </ul>
Delete an access level	<ul style="list-style-type: none"> <li>• <b>View</b> and <b>Delete</b> rights on the access level</li> </ul>
Clone an access level	<ul style="list-style-type: none"> <li>• <b>View</b> right on the access level</li> <li>• <b>Copy</b> right on the access level</li> <li>• <b>Add</b> right on the <b>Access Levels</b> top-level folder</li> </ul>

### 5.3.1 Choosing between View and View On Demand access levels

When reporting over the web, the choice to use live or saved data is one of the most important decisions you'll make. Whichever choice you make, however, Information platform services 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.

## **5.3.2 To copy an existing access level**

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

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

#### **Tip:**

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

3. Click **Organize > Copy**.

A copy of the access level you selected appears in the Details panel.

### 5.3.3 To create a new access level

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

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

### 5.3.4 To rename an access level

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

### 5.3.5 To delete an access level

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

**Note:**

You cannot delete predefined access levels.

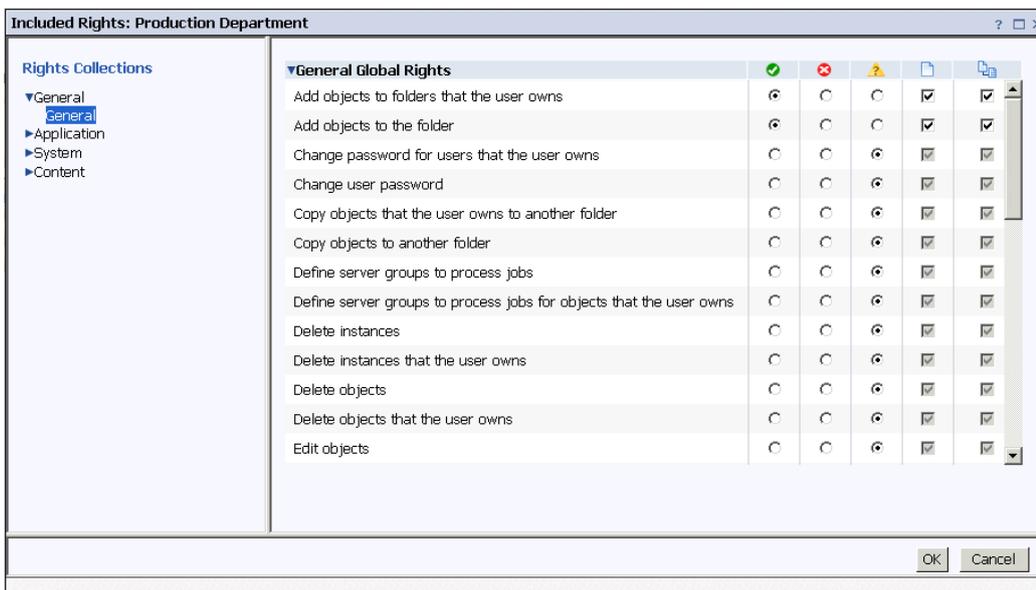
A dialog box appears with information about the objects that this access level affects. If you do not want to delete the access level, click **Cancel** to exit the dialog box.

3. Click **Delete**.  
The access level is deleted, and you return to the "Access Levels" area.

### 5.3.6 To modify rights in an access level

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

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



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

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

#### Related Topics

- [Managing security settings for objects in the CMC](#)

- [Type-specific rights](#)

### 5.3.7 Tracing the relationship between access levels and objects

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

Relationship queries are useful for rights management because they allow you to see objects impacted by an access level in one convenient location. Consider a situation in which a company restructures its organization and merges two departments, Department A and Department B, into Department C. The administrator decides to delete the access levels for Department A and Department B because these departments no longer exist. The administrator runs relationship queries for both access levels before deleting them. In the "Query Results" area, the administrator can see the objects that will be affected if the administrator deletes the access levels. The Details panel also shows the administrator the location of the objects in the CMC if the rights on the objects must be modified before the access levels are deleted.

**Note:**

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

### 5.3.8 Managing access levels across sites

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

**Note:**

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

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

### Modifying replicated access levels in the Origin site

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

#### **Note:**

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

### Modifying replicated access levels in the Destination site

#### **Note:**

This applies to one-way replication only.

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

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

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

#### **Related Topics**

- [Tracing the relationship between access levels and objects](#)

## 5.4 Breaking inheritance

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

#### **Note:**

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

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

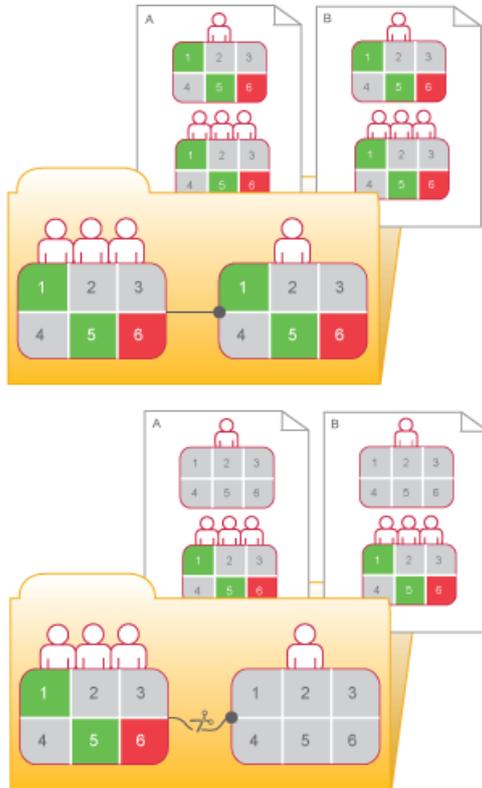


Figure 5-9: Breaking inheritance

### 5.4.1 To disable inheritance

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

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

4. Configure your inheritance settings.

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

5. Click **OK**.

## 5.5 Using rights to delegate administration

Besides allowing you to control access to objects and settings, rights allow you to divide administrative tasks between functional groups within your organization. For example, you may want people from different departments to manage their own Information platform services users and groups. Or you may have one administrator who handles high-level management of Information platform services, 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.

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

Table 5-3: Rights for delegated administrators

Action for delegated administrator	Rights required by the delegated administrator
Create new users	<b>Add</b> right on the top-level <b>Users</b> folder
Create new groups	<b>Add</b> right on the top-level <b>User Groups</b> folder
Delete any controlled groups, as well as individual users in those groups	<b>Delete</b> right on relevant groups
Delete only users that the delegated administrator creates	<b>Owner Delete</b> right on the top-level <b>Users</b> folder
Delete only users and groups that the delegated administrator creates	<b>Owner Delete</b> right on the top-level <b>User Groups</b> folder

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

### 5.5.1 Choosing between “Modify the rights users have to objects” options

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

**Rights Inheritance Settings** right instead of the **Modify Rights Inheritance Settings** right. The differences between these rights are summarized below.

#### **Modify the rights users have to objects**

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

#### **Securely modify the rights users have to objects**

This right allows a user to grant, deny, or revert to unspecified only the rights he is already granted. For example, if user A has **View** and **Securely modify the rights users have to objects** rights, user A 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.

## 5.5.2 Owner rights

Owner rights are rights that apply only to the owner of the object on which rights are being checked. In Information platform services, 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.

## 5.6 Summary of recommendations for rights administration

Keep these considerations in mind for rights administration:

- Use access levels wherever possible. These predefined sets of rights simplify administration by grouping together rights associated with common user needs.
- Set rights and access levels on top-level folders. Enabling inheritance will allow these rights to be passed down through the system with minimal administrative intervention.
- Avoid breaking inheritance whenever possible. By doing so, you can reduce the amount of time it takes to secure the content that you have added to Information platform services.
- 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 Information platform services. After installation, it is recommended that you review the rights of Everyone group members and assign security accordingly.



# Securing Information platform services

## 6.1 Security overview

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

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

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

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

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

## 6.2 Disaster recovery planning

Certain steps must be taken to protect your organization's investment in Information platform services to ensure maximum continuity of function lines of business in the event of a disaster. This section provides guidelines for drafting a disaster recovery plan for your organization.

### General guidelines

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

### Specific guidelines

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

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

## 6.3 General recommendations for securing your deployment

The following are recommended guidelines for securing your Information platform services deployments.

- Use firewalls to protect the communication between the CMS and other system components. If possible, always hide your CMS behind the firewall. At the very least, ensure that the system database is safely behind the firewall.
- Add additional encryption to the File Repository Servers. Once the system is up and running, proprietary content will be stored in these servers. Add additional encryption through the OS or use a third party tool.
- Deploy a reverse proxy server in front of the web application servers in order to hide them behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, therefore hiding private IP addresses.
- Strictly enforce corporate password policies. Ensure that user passwords are routinely changed.
- If you have opted to install the system database and web application server provided with Information platform services, you should access the relevant documentation to ensure these components are deployed with adequate security configurations.
- Use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your deployment.
- Access to the Central Management Console (CMC) should be restricted to local access only. For information on deployment options for the CMC see the *SAP BusinessObjects Enterprise Web Application Deployment Guide*.

### Related Topics

- [Configuring the SSL protocol](#)
- [Password restrictions](#)
- [Configuring security for bundled third-party servers](#)

## 6.4 Configuring security for bundled third-party servers

If you have opted to install third-party server components that are bundled with Information platform services, it is recommended that you access and review the documentation for the following bundled components:

- Microsoft SQL Server 2008 Express Edition: For detailed information on securing this system database for Windows platforms see <http://msdn.microsoft.com/en-us/library/bb283235%28v=sql.100%29.aspx>.
- IBM DB2 Workgroup Edition: For detailed information on securing this system database for UNIX platforms see [http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?nav=/2\\_](http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?nav=/2_).
- Apache Tomcat 6.0: For detailed information on security for this web application server see <http://tomcat.apache.org/tomcat-6.0-doc/index.html>.

## 6.5 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 Information platform services 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 Information platform services components can process the user's requests and actions without prompting for credentials. As such, the active trust relationship provides the basis for Information platform services's distributed security.

### 6.5.1 Logon tokens

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

- **Number of minutes**  
This attribute restricts the lifetime of the logon token.
- **Number of logons**

This attribute restricts the number of times that the logon token can be used to log on to Information platform services .

Both attributes hinder malicious users from gaining unauthorized access to Information platform services 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 Information platform services, the default is to have logon tokens enabled in the web client, however, you can disable logon tokens for BI launch pad. When you disable the logon tokens in the client, the user session will be limited by the web server or web browser timeout. When that session expires, the user will be required to log in to Information platform services again.

## 6.5.2 Ticket mechanism for distributed security

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

Information platform services 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 Information platform services, the ticket is referred to as the logon token.

This logon token is most commonly used over the Web. When users are first authenticated by Information platform services they receive logon tokens from the CMS. The user's web browser caches this logon token. When the user makes a new request, other Information platform services components can read the logon token from the user's web browser.

## 6.6 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.

Information platform services 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 Information platform services logon token is an example of this method.
- **Session variables**—A session variable is a portion of memory that stores session state on the server side. When Information platform services 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, Information platform services implements session tracking.

## 6.6.1 CMS session tracking

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

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

## 6.7 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 Information platform services, environment protection is divided into two areas of communication: web browser to web server, and web server to Information platform services.

### **6.7.1 Web browser to web server**

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

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

**Note:**

These tasks are typically handled by web servers through various security mechanisms, including the Secure Sockets Layer (SSL) protocol, and other such mechanisms. It is good practice to use Secure Sockets Layer (SSL) to reduce security risk between the browser and application or web server.

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

### **6.7.2 Web server to Information platform services**

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

## **6.8 Auditing security configuration modifications**

Any changes to default security configurations for the following will not be audited by SAP BusinessObjects Enterprise:

- Properties files for the web applications (BOE, web services)
- TrustedPrincipal.conf
- Customization performed on BI launch pad and Open Document

In general, any security configuration modifications performed outside the CMC will not be audited. This also applies to modifications performed through the Central Configuration Manager (CCM). Changes committed through the CMC can be audited.

## 6.9 Auditing web activity

Information platform services 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.

### 6.9.1 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.

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

### 6.9.2 Password restrictions

Password restrictions ensure that users authenticating the default Enterprise authentication 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.

### 6.9.3 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, Information platform services has an internal mechanism that enforces a time delay (0.5–1.0 second) between logon attempts. In addition, Information platform services 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)

### 6.9.4 User restrictions

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

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

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

### 6.9.5 Guest account restrictions

The Information platform services authentication provider supports anonymous single sign-on for the Guest account. Thus, when users connect to Information platform services 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.

## 6.10 Processing extensions

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

Through its support for processing extensions, the Information platform services 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 Information platform services environment.

### **Tip:**

By enabling processing extensions, you configure the appropriate Information platform services 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.

## 6.11 Overview of Information platform services data security

Administrators of Information platform services systems manage the way sensitive data is secured through the following:

- A security setting at the cluster level that determines which applications and clients can access the CMS. This setting is managed through the Central Configuration Manager.
- A two-key cryptography system that controls both access to the CMS repository, and keys used to encrypt/decrypt objects within the repository. Access to the CMS repository is set via the Central Configuration Manager, while the Central Management Console has a dedicated management area for cryptographic keys.

These features allow administrators to set Information platform services deployments to particular data security compliance levels and to manage encryption keys used to encrypt and decrypt data within the CMS repository.

## 6.11.1 Data processing security modes

Information platform services can operate in two possible data processing security modes:

- The default data processing security mode. In certain instances, systems running in this mode will use hard-coded encryption keys and do not follow a specific standard. The default mode enables backward compatibility with previous versions of Information platform services client tools and applications.
- A data security mode designed to meet guidelines stipulated by the Federal Information Processing Standard (FIPS) - specifically FIPS 140-2. In this mode FIPS-compliant algorithms and cryptographic modules are used to protect sensitive data. When Information platform services runs in FIPS-compliant mode, all clients tools and applications that do not meet FIPS guidelines are automatically disabled. Information platform services 4.0 client tools and applications are designed to meet the FIPS 140-2 standard. Older clients and applications will not work when Information platform services 4.0 is running in FIPS-compliant mode.

The data processing mode is transparent to system users. In both data processing security modes, sensitive data is encrypted and decrypted in the background by an internal encryption engine.

It is recommended that you use the FIPS-compliant mode in the following circumstances:

- Your Information platform services deployment will not need to use or interact with any legacy client tools or applications.
- Your organization's data processing standards and guidelines prohibit the use of hard-coded encryption keys.
- Your organization is required to secure sensitive data according to FIPS 140-2 regulations.

The data processing security mode is set through the Central Configuration Manager on both Windows and UNIX platforms. Every node in a clustered environment must be set to the same mode.

### 6.11.1.1 To turn on FIPS-compliant mode on Windows

By default, FIPS-compliant mode is off after Information platform services is installed. Use the instructions below to turn on the FIPS-compliant setting for all nodes in your deployment.

1. To start the CCM, choose **Programs > SAP BusinessObjects BI platform 4 > SAP BusinessObjects BI platform > Central Configuration Manager**.
2. In the CCM, right-click the Server Intelligence Agent (SIA) and choose **Stop**.

**Caution:**

Do not proceed to step 3 until the SIA status is marked as Stopped.

3. Right-click the SIA and choose **Properties**.  
The "Properties" dialog box appears, displaying the **Properties** tab.

4. Add `-fips` to the **Command** field, and click **Apply**.
5. Click **OK** to close the "Properties" dialog box.
6. Restart the SIA.

The SIA is operating in FIPS-complaint mode.

You must turn on the FIPS-compliant setting on all SIAs in your Information platform services deployment.

### 6.11.1.2 To turn on FIPS-compliant mode on Unix

All nodes in your Information platform services deployment must be stopped before attempting the following procedure.

By default, FIPS-compliant mode is off after Information platform services is installed. Use the instructions below to turn on the FIPS-compliant setting for all nodes in your deployment.

1. Go to the directory where Information platform services is installed on your Unix computer.
2. Change to the `sap_bobj` directory.
3. Type `ccm.config` and press **Enter**.

The `ccm.config` file is loaded.

4. Add `-fips` to the to the node launch command parameter.

The node launch command parameter appears as `[node nameLaunch]`.

5. Save your changes and **Exit**.
6. Restart the node.

The node is now operating in FIPS-complaint mode.

You must turn on the FIPS-compliant setting on all the nodes in your Information platform services deployment.

### 6.11.1.3 To turn off FIPS-compliant mode on Windows

All servers in your Information platform services deployment must be stopped before attempting the following procedure.

If your deployment is running on FIPS-compliant mode, use the following instructions to turn off the setting.

1. In the CCM, right-click the Server Intelligence Agent (SIA) and choose **Stop**.

**Caution:**

Do not proceed to step 2 until the node status is marked as Stopped.

2. Right-click the SIA and choose **Properties**.  
The "Properties" dialog box appears, displaying the **Properties** tab.
3. Remove `-fips` from the "Command" field and click **Apply**.
4. Click **OK** to close the "Properties" dialog box.
5. Restart the SIA.

## 6.12 Cryptography in Information platform services

### Sensitive Data

Information platform services cryptography is designed to protect sensitive data stored in the CMS repository. Sensitive data includes user credentials, data source connectivity data, and any other info objects that store passwords. This data is encrypted to ensure privacy, keep it free from corruption, and maintain access control. All the requisite encryption resources (including the encryption engine, RSA libraries) are installed by default on each Information platform services deployment.

Information platform services uses a two-key cryptography system.

### Cryptographic Keys

Encryption and decryption of sensitive data is handled in the background through the SDK interacting with the internal encryption engine. System administrators manage data security through symmetric encryption keys without directly encrypting or decrypting specific data blocks.

In the Information platform services system, symmetric encryption keys known as Cryptographic Keys are used to encrypt/decrypt sensitive data. The Central Management Console has a dedicated management area for cryptographic keys. Use the "Cryptographic Keys" to view, generate, deactivate, revoke, and delete keys. The system ensures that any key required to decrypt sensitive data cannot be deleted.

### Cluster Keys

Cluster keys are symmetric key wrapping keys that protect cryptographic keys stored in the CMS repository. Using symmetric key algorithms, cluster keys maintain a level of access control to the CMS repository. Each Information platform services node is assigned a cluster key during installation setup. System administrators can use the CCM to reset the cluster key.

### 6.12.1 Working with cluster keys

During the installation setup for Information platform services, an eight character cluster key is created for the Server Intelligence Agent. This key is used to encrypt all the cryptographic keys in the CMS repository. Without the correct cluster key you cannot access the CMS. The cluster key is stored in encrypted format in the `dbinfo` file. In a default Windows installation the file is stored in the following

**directory:** C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64\_x64 . On Unix systems, the file is stored in the platform directory under <INSTALLDIR>/sap\_bobj/enterprise\_xi40/.

Unix platform	Path
AIX	<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/
Linux	<INSTALLDIR>/sap_bobj/enterprise_xi40/ linux_x86/
HP_UX	<INSTALLDIR>/sap_bobj/enterprise_xi40/ hpux_pa-risc/

The file is name in based on the following convention: `_boe_<sia_name>.dbinfo`, where `<sia_name>` is the name of the server intelligence agent for the cluster.

**Note:**

The cluster key for any given node cannot be retrieved from the `dbinfo` file. It is recommended that system administrators take considered and careful measures to protect cluster keys.

Only users with administrative privileges can reset cluster keys. When required, use the CCM to reset the eight-character cluster key for every node your deployment. New cluster keys are automatically used to wrap the cryptographic keys within the CMS repository.

### 6.12.1.1 To reset the cluster key on Windows

Before resetting the cluster key for make sure all servers managed by the Server Intelligence Agent are stopped.

Use the following procedure to reset the cluster key for your node.

1. To start the CCM, choose **Programs > SAP BusinessObjects BI platform 4 > SAP BusinessObjects BI platform > Central Configuration Manager**.
2. In the CCM, right-click the Server Intelligence Agent (SIA) and choose **Stop**.

**Caution:**

Do not proceed to step 3 until the SIA status is marked as Stopped.

3. Right-click the Server Intelligence Agent (SIA) and choose **Properties**.  
The "Properties" dialog box appears.
4. Click the **Configuration** tab.
5. Under "CMS Cluster Key Configuration", click **Change**.  
A warning message appears.
6. Click **Yes** to continue.  
The "Change Cluster Key" dialog box appears.

7. Type the same eight-character key in the **New Cluster Key** box and the **Confirm New Cluster Key** box.

On Windows, cluster keys must contain a combination of uppercase and lowercase characters.

**Note:**

Users can optionally generate a random key. A random key is required to be FIPS-compliant.

8. Click **OK** to submit the new cluster key to the system.  
A message appears, confirming that the cluster key has been reset successfully.
9. Restart the SIA.

In a multi-node cluster, you must reset the cluster keys for all SIAs in your Information platform services deployment to the new key.

### 6.12.1.2 To reset the cluster key on UNIX

Before resetting the cluster key for a node, make sure all servers managed by the node have been stopped.

1. Go to the directory where Information platform services is installed on your UNIX machine.
2. Change to the `sap bobj` directory.
3. Type `cmsdbsetup.sh` and press **Enter**.  
The "CMS Database Setup" screen appears.
4. Type the name of the node and press **Enter**.
5. Type `2` to change the cluster key.  
A warning message appears.
6. Select **Yes** to continue.
7. In the field provided, type an eight-character new cluster key and press **Enter**.

**Note:**

On UNIX platforms, a valid cluster key contains any combination of eight characters without restrictions.

8. Re-enter the new cluster key in the field provided and press **Enter**.  
A message appears, informing you that the cluster key has been successfully reset.
9. Restart the node.

You must reset all the nodes in your Information platform services deployment to use the same cluster key.

## 6.12.2 Cryptographic Officers

To manage cryptographic keys in the CMC you must be a member of the Cryptographic Officers group. The default administrator account created for Information platform services is also a member of the Cryptographic Officers group. Use this account to add users to the Cryptographic Officers group as required. It is recommended that membership to the group be restricted to a limited number of users.

**Note:**

When users are added to the Administrators group, they do not inherit the rights required to perform management tasks on cryptographic keys.

### 6.12.2.1 To add a user to the Cryptographic Officers group

A user account must exist in the Information platform services system before it can be added to the Cryptographic Officers group.

**Note:**

You must be a member of both of the Administrators and Cryptographic Officers groups to add a user to the Cryptographic Officers group.

1. In the "Users and Groups" management area of the CMC, select the **Cryptographic Officers** group.
2. Click **Actions > Add Members to Group**.  
The "Add" dialog box appears.
3. Click **User list**.  
The **Available users/groups** list refreshes and displays all user accounts in the system.
4. Move the user account that you want to add to the Cryptographic Officers group from the **Available users/groups** list to the **Selected users/groups** list.

**Tip:**

To search for a specific user, use the search field.

5. Click **OK**.

As a member of the Cryptographic Officers group, the newly added account will have access to the "Cryptographic Keys" management area in the CMC.

### 6.12.2.2 To view cryptographic keys in the CMC

The CMC application contains a dedicated management area for cryptographic keys used by the Information platform services system. Access to this area is restricted to members of the Cryptographic Officers group.

1. To start the CMC, choose **Programs > SAP BusinessObjects BI platform 4 > SAP BusinessObjects BI platform > SAP BusinessObjects BI platform Central Management Console**.  
The CMC home page opens.
2. Click the **Cryptographic Keys** tab.  
The "Cryptographic Keys" management area appears.
3. Double-click the cryptographic key for which you want to see details.

#### Related Topics

- [To view objects associated with a cryptographic key](#)

### 6.12.3 Managing cryptographic keys in the CMC

Cryptographic officers use the "Cryptographic Keys" management area to review, generate, deactivate, revoke, and delete keys used to protect sensitive data stored in the CMS repository.

All cryptographic keys currently defined in the system are listed on the "Cryptographic Keys" management area . Basic information for each key is provided under the headings described in the following table:

Heading	Description
Title	Name identifier of the cryptographic key
Status	The key's current status
Last Change	Date and time stamp for the last change associated with the cryptographic key
Objects	Number of objects associated with the key

#### Related Topics

- [Cryptographic key status](#)
- [To create a new cryptographic key](#)
- [To delete a cryptographic key from the system](#)
- [To revoke a cryptographic key](#)
- [To view objects associated with a cryptographic key](#)
- [To mark cryptographic keys as compromised](#)

### 6.12.3.1 Cryptographic key status

The following table lists all the possible status options for cryptographic keys in the Information platform services system:

Status	Description
Active	Only one cryptographic key can be designated by Active status in the system. This key is used to encrypt current sensitive data that will be stored in the CMS database and to decrypt all objects that appear in its Object List. Once a new cryptographic key is created, the currently active key reverts to the Deactivated status. An key with an Active status cannot be deleted from the system.
Deactivated	A deactivated key can no longer be used to encrypt data. It can, however, be used to decrypt all objects in its Object List. You cannot reactivate a key once it has been deactivated. A key with a Deactivated status cannot be deleted from the system. You must changed a key's status to Revoked before it can be deleted.
Compromised	A cryptographic key that is deemed to be insecure can be assigned the Compromised status. After flagging the key, you can later re-encrypt data objects that are still associated with the key. Once a key is marked as compromised, it must be revoked before it can be deleted from the system.
Revoked	When a cryptographic key is revoked, a process is launched in which all objects currently associated with the key are re-encrypted with the current Active cryptographic key. Once a key is revoked it can safely be deleted from the system. The revocation mechanism ensures that data in the CMS database can always be decrypted. There is no way to reactivate a key once it has been revoked.

Status	Description
Deactivated: Rekeying-in process	Indicates that the cryptographic key is in the process of being revoked. Once the process is complete, the key will have a Revoked status.
Deactivated: Rekeying-suspended	Indicates that the process for revoking a cryptographic key has been suspended. This usually occurs if the process has been deliberately suspended or if a data object associated with the key is not available.
Revoked-Compromised	A key has a Revoked-Compromised status if it has been marked as compromised and all data previously associated with it has been encrypted with another key. When a Deactivated key is marked as compromised, you can not take action or revoke the key. Once a compromised key is revoked, it can be deleted.

### 6.12.3.2 To view objects associated with a cryptographic key

1. Select the key in the "Cryptographic Keys" management area of the CMC.
2. Click **Manage > Properties**.  
The cryptographic key's "Properties" dialog box appears.
3. Click **Object List** in the navigation pane on the left of the "Properties" dialog box.  
All the objects associated with the cryptographic key are listed to the right of the navigation pane.

**Tip:**

Use the search functions to look for a specific object.

### 6.12.3.3 To create a new cryptographic key

**Caution:**

When you create a new cryptographic key, the system automatically deactivates the current "Active" key. Once a key has been deactivated it cannot be restored as the "Active" key.

1. In the "Cryptographic Keys" management area of the CMC, click **Manage > New > Cryptographic Key**.  
The "Create New Cryptographic Key" dialog box opens displaying a warning message.
2. Click **Continue** to create the new cryptographic key.
3. Type the name and a description of the new cryptographic key; click **OK** to save your information.  
The new key is listed as the only active key in the "Cryptographic Keys" management area. The previously "Active" key is now marked as "Deactivated."

All new sensitive data generated and stored in the CMS database will now be encrypted with the new cryptographic key. You have the option to revoke the previous key and re-encrypt all its data objects with the new active key.

### 6.12.3.4 To mark cryptographic keys as compromised

You can mark a cryptographic key as compromised if for some reason a cryptographic key is considered to no longer be secure. This is useful for tracking purposes and you can proceed to identify which data objects are associated with the key. A cryptographic key must be deactivated before it can be marked as compromised.

**Note:**

You can also mark a key as compromised after it has been revoked.

1. Go to the "Cryptographic Keys " management area of the CMC.
2. Select the cryptographic key you want to mark as compromised.
3. Click **Actions > Mark as Compromised**.  
The "Mark as Compromised" dialog box displays a warning message.
4. Click **Continue**.
5. Select one of the following options from the "Mark as Compromised" dialog:
  - **Yes:** launches the process to re-encrypt all data objects that are associated with the compromised key.
  - **No:** the "Mark as Compromised" dialog box is closed and the cryptographic key is marked as "Compromised" in the "Cryptographic Keys" management area.

**Note:**

If you select **No**, sensitive data will continue to be associated with the compromised key. The compromised key will be used by the system to decrypt the associated objects.

#### Related Topics

- [To revoke a cryptographic key](#)
- [Cryptographic key status](#)
- [To view objects associated with a cryptographic key](#)

### 6.12.3.5 To revoke a cryptographic key

A Deactivated cryptographic key can still be used by data objects associated with it. To break the association between the encrypted objects and the deactivated key, you must revoke the key using the following instructions.

1. In the "Cryptographic Keys" management area of the CMC, select the key you want to revoke.
2. Click **Actions > Revoke**.  
The "Revoke key" dialog box appears, displaying a warning message.
3. Click **OK** to revoke the cryptographic key.  
A process starts that encrypts all key objects with the active key. If the key is associated with many data objects, it is marked as Deactivated: Rekeying-In Process, until the re-encryption process is complete.

Once a cryptographic key is revoked, it can be safely removed from the system because no sensitive data objects require the key for decryption.

### 6.12.3.6 To delete a cryptographic key from the system

Before you can delete a cryptographic key from the Information platform services system, you must ensure that no data objects in the system require the key. This restriction ensures that all sensitive data stored in the CMS repository can always be decrypted.

After you have successfully revoked a cryptographic key, use the following instructions to delete the key from the system.

1. Go to the "Cryptographic Keys " management area of the CMC.
2. Select the cryptographic key you want to delete.
3. Click **Manage > Delete** .  
The "Delete key " dialog box displays a warning message.
4. Click **Delete** to remove the cryptographic key from the system.  
The deleted key no longer appears in the "Cryptographic Keys "management area of the CMC.

#### **Note:**

Once a cryptographic key is deleted from the system, it cannot be restored.

#### **Related Topics**

- [To revoke a cryptographic key](#)
- [Cryptographic key status](#)

## 6.13 Configuring servers for SSL

You can use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your Information platform services deployment.

To set up SSL for all server communication, you need to perform the following steps:

- Deploy Information platform services 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 also need to configure them for SSL if you will be connecting to the CMS from these thick clients. 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.

### 6.13.1 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.
- Certificates created for previous versions of Information platform services will not work with this release. These certificates will need to be re-created.

#### 6.13.1.1 To create key and certificate files for a machine

1. Run the `SSLC.exe` command line tool.

The SSLC tool is installed with your Information platform services software. (On Windows, for example, it is installed by default in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64.`)

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 `sslc.cnf` file.

- Place the `cakey.pem` and `cacert.pem` files in the directories specified by `sslc.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 `sslc.cnf` file's `database` setting.

**Note:**

By default, this file is `$dir/index.txt`. The file should 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 `111111111111111111111111111111111111`.

- Create the directory specified by the `sslc.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. Run the following command to decrypt the key in the `privkey.pem` file.

```
sslc rsa -in privkey.pem -out 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 (`passphrase.txt`) 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 (`d:/ssl`)) that can be accessed by the machines in your Information platform services 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.

## 6.13.2 Configuring the SSL protocol

After you create keys and certificates for each machine in your deployment, and store them in a secure location, you need to provide the Central Configuration Manager (CCM) and your web application server with the secure location.

You also need to implement specific steps for configuring the SSL protocol for the web application server and for any machine running a thick-client application.

### 6.13.2.1 To configure the SSL protocol in the CCM

1. In the CCM, right-click the Server Intelligence Agent and choose **Properties**.
2. In the Properties dialog box, click the **Protocol** tab.
3. Make sure **Enable SSL** is selected.
4. Provide the file path for the directory where you stored the key and certificate files.

Field	Description
SSL Certificates Folder	Folder where all the required SSL certificates and files are stored. For example: <code>d:\ssl</code> .
Server SSL Certificate File	Name of the file used to store the server SSL certificate. By default, <code>servercert.der</code> .
SSL Trusted Certificates File	Name of the file with the SSL trusted certificate. By default, <code>cacert.der</code> .
SSL Private Key File	Name of the SSL private key file used to access the certificate. By default, <code>server.key</code> .
SSL Private Key Passphrase File	Name of the text file containing the passphrase used to access the private key. By default, <code>passphrase.txt</code> .

**Note:**

Make sure you provide the directory for the machine that the server is running on.

### 6.13.2.2 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.

Example	Description
<code>Dpassphrase=passphrase.txt</code>	The file that stores the passphrase for the private key.

- If you have an IIS web application server, run the `sslconfig` tool from the command line and follow the configuration steps.

### 6.13.2.3 To configure the thick client

Before performing the following procedure you need to create and save all the required SSL resources (for example, certificates and private keys) in a known directory.

In the procedure below it is assumed that you have followed the instructions for creating the following SSL resources:

SSL resource	
SSL certificates folder	<code>d:\ssl</code>
Server SSL certificate file name	<code>servercert.der</code>
SSL trusted certificate or root certificate file name	<code>cacert.der</code>
SSL private key file name	<code>server.key</code>
File containing passphrase for accessing the SSL private key file	<code>passphrase.txt</code>

Once the above resources have been created, use the following instructions to configure thick client applications such as the Central Configuration Manager (CCM) or the upgrade management tool.

- Make sure the thick-client application is not in operation.

**Note:**

Make sure you provide the directory for the machine that the server is running on.

- Run the `sslconfig.exe` command line tool.

The SSLC tool is installed with your software. (On Windows, for example, it is installed by default in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64.`)

- Type the following command:

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey server.key
-passphrase passphrase.txt -protocol ssl
```

- Restart the thick client application.

## Related Topics

- [To create key and certificate files for a machine](#)

### 6.13.2.3.1 To configure SSL login for translation management tool

To enable users to use SSL login with the translation management tool, information about the SSL resources must be added to the tool's configuration (.ini) file.

1. Locate the `TransMgr.ini` file in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
2. Using a text editor, open the `TransMgr.ini`.
3. Add the following parameters:

```
-Dbusinessobjects.orb.ocj.protocol=ssl -DcertDir=D:\SSLCert
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Save the file and close the text editor.

Users can now use SSL to log into the translation management tool.

### 6.13.2.3.2 To configure SSL for report conversion tool

Before performing the following procedure you need to create and save all the required SSL resources (for example, certificates and private keys) in a known directory. In addition, the report conversion tool must be installed as part of your SAP BusinessObjects Enterprise deployment.

In the procedure below it is assumed that you have followed the instructions for creating the following SSL resources:

SSL resource	
SSL certificates folder	d:\ssl
Server SSL certificate file name	servercert.der
SSL trusted certificate or root certificate file name	cacert.der
SSL private key file name	server.key
File containing passphrase for accessing the SSL private key file	passphrase.txt

Once the above resources have been created, use the following instructions to configure SSL to work with the report conversion tool.

1. Create a Windows environment variable `BOBJ_MIGRATION` on the machine hosting the report conversion tool.

**Tip:**

The variable can be set to any value.

2. Using a text editor, open the `migration.bat` in the following directory:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\.
```

3. Located the following line:

```
start "" "%JRE%\bin\javaw" -Xmx512m -Xss10m -jar "%SHAREDIR%\lib\migration.jar"
```

4. Add the following after the -Xss10m parameter:

```
-Dbusinessobjects.oci.protocol=ssl  
-DcertDir=C:/ssl  
-DtrustedCert=cacert.der  
-DsslCert=servercert.der  
-DsslKey=server.key  
-Dpassphrase=passphrase.txt  
-Dbusinessobjects.migration
```

**Note:**

Ensure there is a space between each parameter.

5. Save the file and close the text editor.

Users can now use SSL to access the report conversion tool.

## 6.14 Understanding communication between Information platform services components

If your Information platform services system is deployed entirely on the same secured subnet, there is no need to perform any special configuration of your firewalls. However, you might choose to deploy some components on different subnets separated by one or more firewalls.

It is important to understand the communication between Information platform services servers, rich clients, and the web application server hosting the Information platform services SDK before configuring your system to work with firewalls.

**Related Topics**

- [Configuring BI platform for firewalls](#)
- [Examples of typical firewall scenarios](#)

### 6.14.1 Overview of Information platform services servers and communication ports

It is important to understand Information platform services servers and their communication ports if the Information platform services system is deployed with firewalls.

### 6.14.1.1 Each Information platform services server binds to a Request Port

An Information platform services server, the Input File Repository Server for example, binds to a Request Port when it starts. Other Information platform services components including servers, rich clients, and the SDK hosted in the web application server can use this Request Port to communicate with the server.

A server will select its Request Port number dynamically when the server starts or restarts, unless it is configured to use a specific port number. A specific Request Port number must be configured for servers that communicate with other Information platform services components across a firewall.

### 6.14.1.2 Each Information platform services server registers with the CMS

Information platform services 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.

### 6.14.1.3 Central Management Server provides a directory of registered services

The Central Management Server (CMS) provides a directory of the Information platform services services that have registered with it. Other Information platform services components such as services, rich clients, and the SDK hosted in the web application server can contact the CMS and request a reference to a particular service. A service's reference contains the service's Request Port number and the host name (or IP address) of the server's host computer and service ID.

Information platform services components might reside on a different subnet than the server they are using. The host name (or IP address) contained in the service's reference must be routable from the component's computer.

**Note:**

The reference to an Information platform services server will contain the server computer's host name by default. (If a computer has more than one hostname, the primary hostname is chosen). You can configure a server so that its reference contains the IP address instead.

**Related Topics**

- [Communication between Information platform services components](#)

#### 6.14.1.4 The CMS uses two ports

The CMS uses two ports: the Request Port and the Name Server Port. The Request Port is selected dynamically by default. The Name Server Port is 6400 by default.

All Information platform services servers and client applications will initially contact the CMS on its Name Server port. The CMS will respond to this initial contact by returning the value of its Request Port. The servers will use this Request Port for subsequent communication with the CMS.

#### 6.14.1.5 Server Intelligence Agents (SIA) communicate with the Central Management Server (CMS)

Your deployment will not work if the Server Intelligence Agent (SIA) and Central Management Server (CMS) cannot communicate with each other. Ensure that your firewall ports are configured to allow communication between all SIAs and all CMSs in the cluster.

#### 6.14.1.6 Job server child processes communicate with the data tier and the CMS

Most job servers create a child process to handle a task such as generating a report. The job server 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 by adding the `-requestJSChildPorts<lowestport>-<highestport>` and `-requestPort<port>` parameters to the server's command line. Note that the port range should be large enough to allow the maximum number of child process as specified by `-maxJobs`.
- Open the specified port range on the firewall.

Many child processes communicate with the data tier. For example, a child process might connect to a reporting database, extract data, and calculate values for a report. If the job server child process communicates with the data tier across a firewall, you must:

- Open a communicate path on the firewall from any port on the job server machine to the database listen port on the database server machine.

**Related Topics**

- [Command lines overview](#)

## 6.14.2 Communication between Information platform services components

Information platform services components, such as browser clients, rich clients, servers, and the SDK hosted in the web application server, communicate with each other across the network during typical workflows. You must understand these workflows to deploy SAP BusinessObjects products across different subnets that are separated by a firewall.

### 6.14.2.1 Requirements for communication between Information platform services components

Deployments of Information platform services must conform to these general requirements.

1. Every server must be able to initiate communication with every other Information platform services server on that server's Request Port.
2. The CMS uses two ports. Every Information platform services server, Information platform services rich client, and the web application server that hosts the Information platform services 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 communicate with the CMS.
4. Thick clients must be able to initiate communication with the Request Port of the Input and Output File Repository Servers
5. If auditing is enabled for thick clients and web applications they must be able to initiate communication with the Request Port of the Adaptive Processing Servers that hosts the Client Auditing Proxy Service.
6. In general, the web application server that hosts the Information platform services SDK must be able to communicate with the Request Port of every Information platform services server.

**Note:**

The web application server only needs to communicate with Information platform services servers that are used in the deployment. For example, if Crystal Reports is not being used, the web application server does not need to communicate with the Crystal Reports Cache Servers.

7. Job Servers use the port numbers that are specified with the `-requestJSChildPorts <port range>` command. If no range is specified in the command line, the servers use random port numbers. To allow a job server to communicate with a CMS, FTP, or mail server on another machine open all of the ports in the range specified by `-requestJSChildPorts` on your firewall.
8. The CMS must be able to communicate with the CMS database listen port.

9. The Connection Server, most Job Server child process, and every system database and auditing Processing Server must be able to initiate communication with the reporting database listen port.

**Related Topics**

- [Information platform services port requirements](#)

### 6.14.2.2 Information platform services port requirements

This section lists the communication ports used by Information platform services servers, thick clients, the web application server hosting the SDK, and third-party software applications. If you deploy Information platform services with firewalls, you can use this information to open the minimum number of ports in those firewalls.

#### 6.14.2.2.1 Port Requirements for Information platform services applications

This table lists the servers and port numbers used by Information platform services applications.

Product	Client Application	Associated Servers	Server Port Requirements
Crystal Reports	SAP Crystal Reports 2011 designer	CMS Input FRS Output FRS Crystal Reports 2011 Report Application Server (RAS) Crystal Reports 2011 Processing Server Crystal Reports Cache Server	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port Crystal Reports 2011 Report Application Server Request Port Crystal Reports 2011 Processing Server Request Port Crystal Reports Cache Server Request Port

Product	Client Application	Associated Servers	Server Port Requirements
Crystal Reports	SAP Crystal Reports for Enterprise designer	CMS Input FRS Output FRS Crystal Reports Processing Server Crystal Reports Cache Server	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port Crystal Reports Processing Server Request Port Crystal Reports Cache Server Request Port
Dashboards	SAP BusinessObjects Dashboards	CMS Input FRS Output FRS Web Services provider application ( <code>dswsbobje.war</code> ) that hosts the Dashboards, Live Office, and QaaWS web services required for certain data source connections	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port HTTP port (80 by default)
Live Office	Live Office Client	Web Services provider application ( <code>dswsbobje.war</code> ) that hosts the Live Office web service	HTTP port (80 by default)
Information platform services	SAP BusinessObjects Web Intelligence Desktop	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
Information platform services	Universe design tool	CMS Input FRS Connection Server	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Connection Server port
Information platform services	Business View Manager	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port
Information platform services	Central Configuration Manager (CCM)	CMS Server Intelligence Agent (SIA)	The following ports must be open to allow CCM to manage remote Information platform services servers: CMS Name Server Port (6400 by default) CMS Request Port The following ports must be open to allow CCM to manage remote SIA processes: Microsoft Directory Services (TCP port 445) NetBIOS Session Service (TCP port 139) NetBIOS Datagram Service (UDP port 138) NetBIOS Name Service (UDP port 137) DNS (TCP/UDP port 53) (Note that some ports listed above may not be required. Consult your Windows administrator).

Product	Client Application	Associated Servers	Server Port Requirements
Information platform services	Server Intelligence Agent (SIA)	Every Information platform services server including the CMS	SIA Request Port (6410 by default) CMS Name Server Port (6400 by default) CMS Request Port
Information platform services	Report Conversion Tool	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port
SAP Business Objects Enterprise	Repository Diagnostic Tool	CMS Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port
SAP Business Objects Information platform services	Information platform services SDK hosted in the web application server	All Information platform services servers required by the deployed products.  For example, communication with the Crystal Reports 2011 Processing Server Request Port is required if the SDK is retrieving and interacting with Crystal reports from the CMS.	CMS Name Server Port (6400 by default) CMS Request Port  Request Port for each server that is required. For example, the Crystal Reports 2011 Processing Server Request Port.

Product	Client Application	Associated Servers	Server Port Requirements
SAP Business Objects Information platform services	Web Services provider (dswsbobje.war)	<p>All Information platform services servers required by the products accessing the web services.</p> <p>For example, communication with the Dashboards Cache and Processing Server Request Ports is required if SAP BusinessObjects Dashboards is accessing Enterprise data source connections through the Web Services provider.</p>	<p>CMS Name Server Port (6400 by default)</p> <p>CMS Request Port</p> <p>Request Port for each server that is required. For example, the Dashboard Design Cache Server and Dashboard Design Processing Server Request Ports.</p>
SAP Business Objects Information platform services	SAP BusinessObjects Analysis, edition for OLAP	<p>CMS</p> <p>Adaptive Processing Server hosting the Multi Dimensional Analysis Service</p> <p>Input FRS</p> <p>Output FRS</p>	<p>CMS Name Server Port (6400 by default)</p> <p>CMS Request Port</p> <p>Adaptive Processing Server Request Port</p> <p>Input FRS Request Port</p> <p>Output FRS Request Port</p>

6.14.2.2.2 Port Requirements for Third-Party Applications

This table lists third-party software used by SAP Business Objects products. It includes specific examples from some software vendors, but different vendors will have different port requirements.

Third-party application	SAP Business Objects component that uses the third-party product	Third-party application port requirement	Description
CMS System Database	Central Management Server (CMS)	Database server listen port	The CMS is the only server that communicates with the CMS system database.

Third-party application	SAP Business Objects component that uses the third-party product	Third-party application port requirement	Description
CMS Auditing Database	Central Management Server (CMS)	Database server listen port	The CMS is the only server that communicates with the CMS auditing database.
Reporting Database	Connection Server Every Job Server child process Every Processing Server	Database server listen port	These servers retrieve information from the reporting database.
web application server	All SAP Business Objects web services and web applications including BI launch pad and CMC	HTTP port and HTTPS port. For example, on Tomcat the default HTTP port is 8080 and the default HTTPS port is 443.	The HTTPS port is only required if secure HTTP communication is used.
FTP server	Every Job Server	FTP In (port 21) FTP Out (port 22)	The Job Servers use the FTP ports to allow <b>send to FTP</b> .
Email server	Every Job Server	SMTP (port 25)	The Job Servers use the SMTP port to allow <b>send to email</b> .
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 <b>send to disk</b> .

Third-party application	SAP Business Objects component that uses the third-party product	Third-party application port requirement	Description
Authentication Server	CMS web application server that hosts the Information platform services SDK every thick Client, for example Live Office.	Connection port for third-party authentication. For example, the connection server for the Oracle LDAP server is defined by the user in the file ldap.ora.	User credentials are stored in the third-party authentication server. The CMS, Information platform services SDK, and the thick clients listed here need to communicate with the third-party authentication server when a user logs on.

## 6.15 Configuring BI platform for firewalls

This section gives step-by-step instructions for configuring your BI platform system to work in a firewalled environment.

### 6.15.1 To configure the system for firewalls

1. Determine which Information platform services components must communicate across a firewall.
2. Configure the Request Port for each Information platform services server that must communicate across a firewall.
3. Configure a port range for any Job Server children that must communicate across a firewall by adding the `-requestJSChildPorts<lowestport>-<highestport>` and `-requestPort<port>` parameters to the server's command line.
4. Configure the firewall to allow communication to the Request Ports and job server port range on the Information platform services servers that you configured in the previous step.
5. (Optional) Configure the hosts file on each machine that hosts a Information platform services server that must communicate across a firewall.

#### Related Topics

- [Communication between Information platform services components](#)
- [Configuring port numbers](#)
- [Command lines overview](#)

- [Specifying the firewall rules](#)
- [Configure the hosts file for firewalls that use NAT](#)

### 6.15.1.1 Specifying the firewall rules

You must configure the firewall to allow the necessary traffic between SAP BusinessObjects 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 SAP BusinessObjects 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 Information platform services is deployed across firewalls that use NAT, every server on all machines needs a unique Request Port number. That is, no two servers in the entire deployment can share the same Request Port.

**Note:**

You do not need to specify any outbound access rules. Information platform services servers do not initiate communication to the web application server, or to any client applications. Information platform services servers can initiate communication to other Information platform services servers in the same cluster. Deployments with clustered servers in an outbound-firewalled environment are not supported.

**Example:**

This example shows the inbound access rules for a firewall between the web application server and the Information platform services 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

Source Computer	Port	Destination Computer	Port	Action
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 Information platform services servers	Any	Reject

**Related Topics**

- [Configure the hosts file for firewalls that use NAT](#)

**6.15.1.2 Configure the hosts file for firewalls that use NAT**

This step is required only if the Information platform services servers must communicate across a firewall on which Network Address Translation (NAT) is enabled. This step allows the client machines to map a server's hostname to a routable IP address.

**Note:**

Information platform services 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.

Information platform services components such as servers, thick clients, and the web application server hosting the Information platform services SDK will use a service reference to contact a server. The

service reference contains the hostname of the server's machine. This hostname must be routable from the Information platform services component's machine. This means the `hosts` file on the component's machine must map the server machine's hostname to the server machine's external IP address. The server machine's external IP address is routable from external side of the firewall, whereas the internal IP address is not.

The procedure for configuring the `hosts` file is different for Windows and UNIX.

#### 6.15.1.2.1 To configure the hosts file on Windows

1. Locate every machine that runs a Information platform services 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 Information platform services server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

#### 6.15.1.2.2 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 an Information platform services 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 an Information platform services server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

## 6.15.2 Debugging a firewalled deployment

If one or more of your Information platform services servers do not work when your firewall is enabled, even though the expected ports have been opened on the firewall, you can use the event logs to determine which of the servers is attempting to listen on which ports or IP Addresses. You can then either open those ports on your firewall, or use the Central Management Console (CMC) to change the port numbers or IP addresses that these servers attempt to listen on.

Whenever an Information platform services server starts, the server writes the following information to the Event Log for each request port that it attempts to bind to.

- "Server" - The name of the server and whether it successfully started.

- "Published Address(es)" - A list of IP Address and port combinations which are posted to the name service that other servers will use to communicate with this server.

If the server successfully binds to a port, the log file also displays "Listening on port(s)", the IP Address and port that the server is listening on. If the server is unsuccessful in binding to the port, the log file displays "Failed to listed on port(s)", the IP Address and port that the server attempts to listen on and fails.

When a Central Management Server starts, it also writes Published Address(es), Listening on port(s), and Failed To Listen On information for the server's Name Service Port.

**Note:**

If the server is configured to use a port that is auto-assigned and to use a host name or IP Address that is invalid, the event log indicates that the server failed to listen on the host name or IP Address and port "0". If a specified host name or IP Address is invalid, the server will fail before the host operating system is able to assign a port.

**Example:**

The following example shows the an entry for a Central Management Server that is successfully listening on two Request Ports and a Name Service Port.

```
Server mynode.cms1 successfully started.
Request Port :
  Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032, 10.90.172.216:8765
Name Service Port :
  Published Address(es): mymachine.corp.com:6400
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400, 10.90.172.216:6400
```

---

### 6.15.2.1 To debug a firewalled deployment

1. Read the event log to determine if the server is successfully binding to the port that you have specified. If the server was unable to successfully bind to a port, there is probably a port conflict between the server and another process that is running on the same machine. The "Failed to List On" entry indicates the port that the server is attempting to listen on. Run a utility such as netstat to determine which process that has taken the port, and then configure either the other process or the server to listen on another port.
2. If the server was able to successfully bind to a port, "Listening On" indicates which port the server is listening on. If a server is listening on a port and is still not working properly, either ensure that that port is open on the firewall or configure the server so that it listens on a port that is open.

**Note:**

If all of the Central Management Servers in your deployment are attempting to listen to ports or IP Addresses that are not available, then the CMSs will not start and you will not be able to log on to the CMC. If you want to change the port number or IP Address that the CMS attempts to listen, you must use the Central Configuration Manager (CCM) to specify a valid port number or IP Address.

## Related Topics

- [Configuring port numbers](#)

## 6.16 Examples of typical firewall scenarios

This section provides examples of typical firewall deployment scenarios.

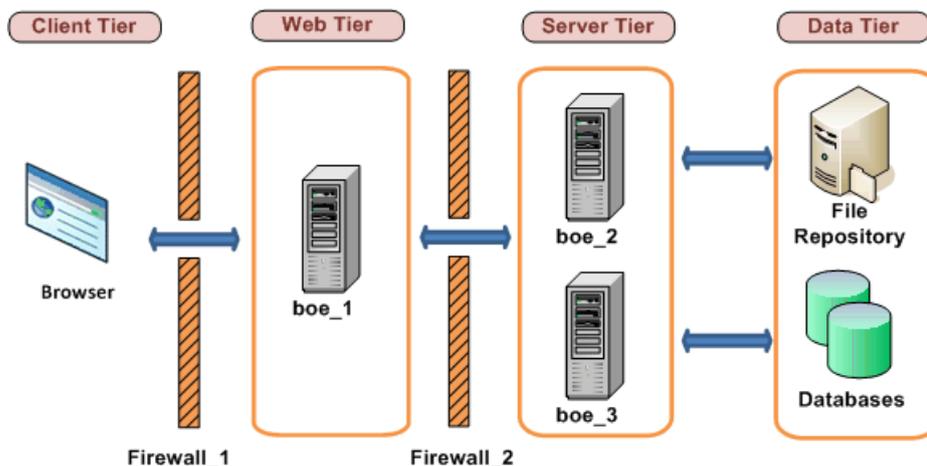
### 6.16.1 Example - Application tier deployed on a separate network

This example shows how to configure a firewall and Information platform services to work together in a deployment where the firewall separates the web application server from other Information platform services servers.

In this example, Information platform services components are deployed across these machines:

- Machine `boe_1` hosts the web application server and the Information platform services SDK.
- Machine `boe_2` hosts the Intelligence tier servers, including the Central Management Server, the Input File Repository Server, the Output File Repository Server, and the Event server.
- Machine `boe_3` hosts the Processing tier servers, including the Adaptive Job Server, the Web Intelligence Processing Server, the Report Application Server, the Crystal Reports Cache Server, and Crystal Reports Processing Server.

Figure 6-1: Application tier deployed on a separate network



### 6.16.1.1 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 Information platform services SDK must be able to communicate with the CMS on both of its ports.
  - The web application server that hosts the Information platform services SDK must be able to communicate with every Information platform services 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 Information platform services servers on machine `boe_2` and `boe_3`. Configure the port numbers for each server on these machines. Note that you can use any free port between 1,025 and 65,535.

The port numbers chosen for this example are listed in the table:

Server	Port Number
Central Management Server	6400
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event server	6425
Adaptive Job Server	6435
Crystal Reports Cache server	6440
Web Intelligence Processing Server	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. Configure the firewalls `Firewall_1` to allow communication to the fixed ports on the Information platform services servers and the web application server that you configured in the previous step. In this example we are opening the HTTP Port for the Tomcat Application server.

Table 6-6: 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
boe_1	Any	boe_3	6460	Allow
boe_1	Any	boe_3	6465	Allow
boe_1	Any	boe_3	6470	Allow

- 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 Information platform services components](#)

## 6.16.2 Example - Thick client and database tier separated from Information platform services servers by a firewall

This example shows how to configure a firewall and Information platform services to work together in a deployment scenario where:

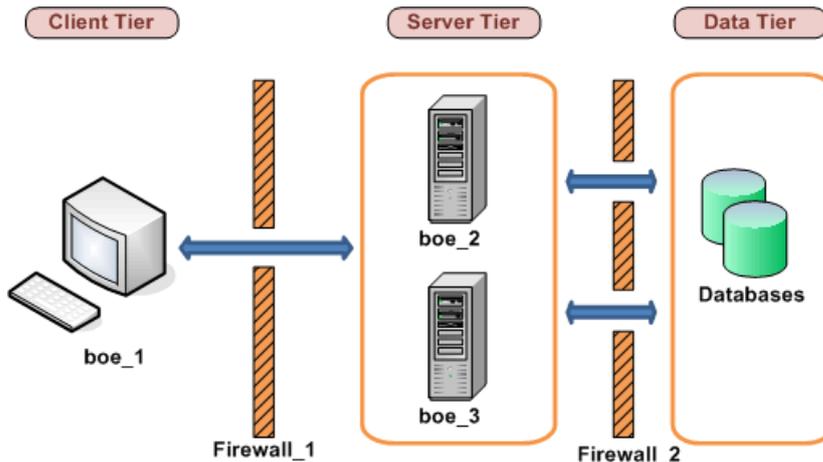
- One firewall separates a thick client from Information platform services servers.

- One firewall separates Information platform services servers from the database tier.

In this example, Information platform services components are deployed across these machines:

- Machine `boe_1` hosts the Publishing Wizard. Publishing Wizard is a Information platform services thick client.
- Machine `boe_2` hosts the Intelligence tier servers, including the Central Management Server (CMS), the Input File Repository Server, the Output File Repository Server, and the Event server.
- Machine `boe_3` hosts the Processing tier servers, including: Adaptive Job Server, Web Intelligence Processing Server, Report Application Server, the Crystal Reports Processing Server, and Crystal Reports Cache Server.
- Machine `Databases` hosts the CMS system and auditing databases and the reporting database. Note that you can deploy both databases on the same database server, or you can deploy each database on its own database server. In this example, all the CMS databases and the reporting database are deployed on the same database server. The database server listen port is 3306, which is the default listen port for MySQL server.

Figure 6-2: Rich client and database tier deployed on separate networks



### 6.16.2.1 To configure tiers separated from Information platform services 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 Information platform services servers that you configured in the previous step. Note that port 6400 is the default port number for the CMS Name Server Port and did not need to be explicitly configured in the previous step.

Port	Destination Computer	Port	Action
Any	boe_2	6400	Allow
Any	boe_2	6411	Allow
Any	boe_2	6415	Allow
Any	boe_2	6416	Allow

Configure *Firewall\_2* to allow communication to the database server listen port. The CMS (on **boe\_2**) must have access to the CMS system and auditing database and the Job Servers (on **boe\_3**) must have access to the system and auditing databases. Note that we did not have configure a port range for job server child processes because their communication with the CMS did not cross a firewall.

Source Computer	Port	Destination Computer	Port	Action
boe_2	Any	Databases	3306	Allow
boe_3	Any	Databases	3306	Allow

5. This firewall is not NAT-enabled, and so we do not have to configure the `hosts` file.

### Related Topics

- [Understanding communication between Information platform services components](#)
- [Configuring BI platform for firewalls](#)

## 6.17 Firewall settings for integrated ERP environments

This section details specific considerations and port settings for Information platform services systems that integrate with the following ERP environments.

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Information platform services components include browser clients, rich clients, servers, and the Information platform services SDK hosted in the Web Application server. System components can be installed on multiple machines. It is useful to understand the basics of communication between Information platform services and the ERP components before configuring you system to work with firewalls

### Port requirements for Information platform services servers

The following ports are required for their corresponding servers in Information platform services:

Server Port Requirements
<ul style="list-style-type: none"> <li>• Central Management Server Name Server port</li> <li>• Central Management Server Request port</li> <li>• Input FRS Request port</li> <li>• Output FRS Request port</li> <li>• Report Application Server Request port</li> <li>• Crystal Reports Cache Server Request port</li> <li>• Crystal Reports Page Server Request port</li> <li>• Crystal Reports Processing Server Request Port</li> </ul>

### 6.17.1 Specific firewall guidelines for SAP integration

Your Information platform services deployment must conform to the following communication rules:

- The CMS must be able to initiate communication with SAP system on SAP System Gateway port.
- The Adaptive Job Server and Crystal Reports Processing Server (along with Data Access components) must be able to initiate communication with SAP system on the SAP System Gateway port.

- The BW Publisher component must be able to initiate communication with the SAP system on the SAP System Gateway port.
- Information platform services components deployed on the SAP Enterprise Portal side (for example, iViews and KMC) must be able to initiate communication with Information platform services web applications on HTTP/HTTPS ports.
- The web application server must be able to initiate communication on the SAP System Gateway service.
- Crystal Reports must be able to initiate communication with the SAP host on the SAP System Gateway port and SAP System Dispatcher port.

The port that the SAP Gateway service is listening on is the same as that specified in the installation.

**Note:**

If a component requires an SAP router to connect to an SAP system, you can configure the component using the SAP router string. For example, when configuring an SAP entitlement system to import roles and users, the SAP router string can be substituted for the application server's name. This insures that the CMS will communicate with the SAP system through the SAP router.

### 6.17.1.1 Detailed port requirements

#### **Port requirements for SAP**

Information platform services uses the SAP Java Connector (SAP JCO) to communicate with SAP NetWeaver (ABAP). You need to configure and ensure the availability of the following ports:

- SAP Gateway service listening port (for example, 3300).
- SAP Dispatcher service listening port (for example, 3200).

The following table summarizes the specific port configurations that you need.

Source computer	Port	Destination computer	Port	Action
SAP	Any	Information platform services Web Application Server	Web Service HTTP/HTTPS port	Allow
SAP	Any	CMS	CMS Name Server port	Allow
SAP	Any	CMS	CMS Requested port	Allow
Web Application Server	Any	SAP	SAP System Gateway Service port	Allow
Central Management Server (CMS)	Any	SAP	SAP System Gateway Service port	Allow
Crystal Reports	Any	SAP	SAP System Gateway Service port and SAP System Dispatcher port	Allow

## 6.17.2 Firewall configuration for JD Edwards EnterpriseOne integration

Deployments of Information platform services that will communicate with JD Edwards software must conform to these general communication rules:

- Central Management Console Web Applications must be able to initiate communication with JD Edwards EnterpriseOne through the JDENET port and a randomly selected port.
- Crystal Reports with Data Connectivity client side component must be able to initiate communication with JD Edwards EnterpriseOne through the JDNET port. For retrieving data, JD Edwards EnterpriseOne side must be able to communicate with the driver through a random port that cannot be controlled.
- Central Management Server must be able to initiate communications with JD Edwards EnterpriseOne through the JDENET port and a randomly selected port.
- The JDENET port number can be found in the JD Edwards EnterpriseOne Application Server configuration file (`JDE.INI`) under the JDENET section.

### 6.17.2.1 Port Requirements for Information platform services servers

Product	Application	Server Port Requirements
Information platform services XI	Information platform services XI	<ul style="list-style-type: none"> <li>Information platform services Sign-on Server port</li> </ul>

### 6.17.2.2 Port Requirements for JD Edwards EnterpriseOne

Product	Port Requirement	Description
JD Edwards EnterpriseOne	JDENET port and a randomly selected port	Used for communication between Information platform services and JD Edwards EnterpriseOne application server.

### 6.17.2.3 Configuring Information platform services Web Application server to communicate with JD Edwards

This section shows how to configure a firewall and Information platform services to work together in a deployment scenario where the firewall separates the Web Application server from other Information platform services servers.

For firewall configuration with Information platform services servers and clients, see the *Information platform services port requirements* section of this guide . In addition to the standard firewall configuration, communication with JD Edwards servers requires some extra ports to be opened.

Table 6-14: For JD Edwards EnterpriseOne Enterprise

Source Computer	Port	Destination Computer	Port	Action
CMS with Security Connectivity feature for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
Information platform services servers with Data Connectivity for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow

Source Computer	Port	Destination Computer	Port	Action
Crystal Reports with client side Data Connectivity for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
Information platform services Web Application Server	Any	JD Edwards EnterpriseOne	Any	Allow

### 6.17.3 Specific firewall guidelines for Oracle EBS

Your deployment of Information platform services must allow the following components to initiate communication with the Oracle database listener port.

- Information platform services web components
- CMS (specifically the Oracle EBS security plugin)
- Information platform services XI backend servers (specifically the EBS Data Access component)
- Crystal Reports (specifically the EBS Data Access component)

**Note:**

The default value of the Oracle database listener port in all the above is 1521.

#### 6.17.3.1 Detailed port requirements

In addition to the standard firewall configuration for Information platform services, some extra ports need to be opened to work in an integrated Oracle EBS environment:

Source Computer	Port	Destination Computer	Port	Action
Web application server	Any	Oracle EBS	Oracle database port	Allow
CMS with security connectivity for Oracle EBS	Any	Oracle EBS	Oracle database port	Allow
Information platform services servers with server-side data connectivity for Oracle EBS	Any	Oracle EBS	Oracle database port	Allow

Source Computer	Port	Destination Computer	Port	Action
Crystal Reports with client-side data connectivity for Oracle EBS	Any	Oracle EBS	Oracle database port	Allow

### 6.17.4 Firewall configuration for PeopleSoft Enterprise integration

Deployments of BusinessObjects XI Integration for PeopleSoft must conform to the following general communication rules:

- The Central Management Server (CMS) with the Security Connectivity component must be able to initiate communication with the PeopleSoft Query Access (QAS) web service.
- Information platform services servers with a Data Connectivity component must be able to initiate communication with the PeopleSoft QAS web service.
- The Crystal Reports with Data Connectivity client components must be able to initiate communication with the PeopleSoft QAS web service.
- The Enterprise Management (EPM) Bridge must be able to communicate with the CMS and the Input File Repository Server.
- the EPM Bridge must be able to communicate with the PeopleSoft database using an ODBC connection.

The web service port number is the same as the port specified in PeopleSoft Enterprise Domain name.

#### 6.17.4.1 Port Requirements for Information platform services XI servers

Product	Application	Server Port Requirements
Information platform services XI Enterprise	Information platform services XI Enterprise	<ul style="list-style-type: none"> <li>• Information platform services Sign-on Server port</li> </ul>

#### 6.17.4.2 Port Requirements for PeopleSoft

Product	Port Requirement	Description
PeopleSoft Enterprise: People Tools 8.46 or newer	Web Service HTTP/HTTPS port	This port is required when using SOAP connection for PeopleSoft Enterprise for People Tools 8.46 and newer solutions

### 6.17.4.3 Configuring BusinessObjects XI Integration for PeopleSoft for firewalls

This section shows how to configure a firewall and Information platform services with Information platform services XI Enterprise to work together in a deployment scenario where the firewall separates the Web Application server from other Information platform services servers.

For firewall configuration with Information platform services servers and clients, refer to the *Information platform services XI Administrator's Guide*.

Besides the firewall configuration with Information platform services, Information platform services XI Enterprise needs to do some extra configurations.

Table 6-18: For PeopleSoft Enterprise: PeopleTools 8.46 or newer

Source Computer	Port	Destination Computer	Port	Action
CMS with Security Connectivity feature for PeopleSoft	Any	PeopleSoft	PeopleSoft web service HTTP /HTTPS port	Allow
Information platform services servers with Data Connectivity for PeopleSoft	Any	PeopleSoft	PeopleSoft web service HTTP /HTTPS port	Allow
CrystalReports with client side Data Connectivity for PeopleSoft	Any	PeopleSoft	PeopleSoft web service HTTP /HTTPS port	Allow
EPM Bridge	Any	CMS	CMS Name Server Port	Allow
EPM Bridge	Any	CMS	CMS requested port	Allow
EPM Bridge	Any	Input File Repository Server	Input FRS port	Allow

Source Computer	Port	Destination Computer	Port	Action
EPM Bridge	Any	PeopleSoft	PeopleSoft Database Port	Allow

### 6.17.5 Firewall configuration for Siebel integration

This section shows which ports are used for communication between Information platform services XI and Siebel eBusiness Application systems when they are separated by firewalls.

- The Web Application must be able to initiate communication with the Information platform services Sign-on Server for Siebel. For enterprise Sign-on Server for Siebel three ports are needed:
  1. The Echo (TCP) port 7 for checking access to the Sign-on Server.
  2. Information platform services Sign-on Server for Siebel port (by default, 8448) for CORBA IOR listening port.
  3. A random POA port for CORBA communication that cannot be controlled, so all ports need to open.
- The CMS must be able to initiate communication with Information platform services Sign-on Server for Siebel. CORBA IOR listening port configured for each Sign-on Server (for example, 8448). You will also need to open a random POA port number that will not be known until you have installed Information platform services.
- Information platform services Sign-on Server for Siebel must be able to initiate communication with SCBroker (Siebel connection broker) port (for example, 2321).
- Information platform services backend servers (Siebel Data Access component) must be able to initiate communication with SCBroker (Siebel connection broker) port (for example, 2321).
- Crystal Reports (Siebel Data Access component) must be able to initiate communication with SCBroker (Siebel connection broker) port (for example, 2321).

#### Detailed description of ports

This section lists the ports that are used by Information platform services XI. If you deploy Information platform services with firewalls, you can use this information to open the minimum number of ports in those firewalls specific for BusinessObjects XI Integration for Siebel.

Table 6-19: Port requirement for Information platform services XI servers

Product	Application	Server Port Requirements
SAP BusinessObjects XI Enterprise	BusinessObjects XI Siebel integration	<ul style="list-style-type: none"> <li>• Information platform services Sign-on Server port</li> </ul>

Table 6-20: Port requirement for Siebel

Product	Port Requirement	Description
Siebel eBusiness Application	2321	Default SCBroker (Siebel connection broker) port

### Configuring SAP Information platform services XI firewalls for integration with Siebel

This section shows how to configure a firewalls for Siebel and Information platform services XI to work together in a deployment scenario where the firewall separates the Web Application server from other Information platform services XI servers.

Source Computer	Port	Destination Computer	Port	Action
Web Application Server	Any	Information platform services Sign-on Server for Siebel	Any	Allow
CMS	Any	Information platform services Sign-on Server for Siebel	Any	Allow
Information platform services Sign-on Server for Siebel	Any	Siebel	SCBroker port	Allow
Information platform services servers with server-side Data Connectivity for Siebel	Any	Siebel	SCBroker port	Allow
Crystal Reports with client-side Data Connectivity for Siebel	Any	Siebel	SCBroker port	Allow

## 6.18 Information platform services and reverse proxy servers

Information platform services 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 Information platform services web applications that are deployed on the internal network.

## 6.18.1 Supported reverse proxy servers

Information platform services supports the following reverse proxy servers:

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

## 6.18.2 Understanding how web applications are deployed

Information platform services web applications are deployed on a web application server. The applications are deployed automatically during installation through the WDeploy tool. WDeploy can also be used to manually deploy the applications after Information platform services is deployed. The web applications are located in the following directory on a default Windows installation:

```
C:\Program Files (x86)\SAP BusinessObjects\Information platform services  
__MINI-BOE-VERSION__\warfiles\webapps
```

WDeploy is used to deploy two specific WAR files:

- **BOE**: includes the Central Management Console (CMC), BI launch pad, Open Document,
- **dswsbobje**: contains the Web Service application

If the web application server is located behind a reverse proxy server, the reverse proxy server should be configured with the correct context paths of the WAR files. To expose all of the Information platform services functionality, configure a context path for every Information platform services WAR file that is deployed.

## 6.19 Configuring reverse proxy servers for Information platform services web applications

The reverse proxy server must be configured to map incoming URL requests to the correct web application in deployments where Information platform services 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.

## 6.19.1 Detailed instructions for configuring reverse proxy servers

### Configure the WAR files

Information platform services web applications are deployed as WAR files on a web application server. Ensure you configure a directive on your reverse proxy server for the WAR file that is required for your deployment. You can use the WDeploy to deploy either the BOE or dswsbobje WAR files. For more information on WDeploy see the *Information platform services Web Application Deployment Guide*.

### Specify BOE properties in the custom configuration directory

The BOE.war file includes global and application specific properties. If you need to modify any of the of properties use the custom configuration directory. By default the directory is located at `C:\Program Files (x86)\SAP BusinessObjects\Information platform services __MINI-BOE-VERSION__\warfiles\webapps\BOE\WEB-INF\config\custom`.

#### Note:

Do not modify the properties in the `config\default` directory. If you make any changes, the changes will overwrite files in the default directory. Ensure that users only use the `config\custom` directory.

#### Note:

On some web application servers, such as the Tomcat version bundled with Information platform services, you can access the BOE.war file directly. In this scenario, you can set custom settings without undeploying the WAR file. When you cannot access the BOE.war file, you must undeploy, customize, and then redeploy the file.

### Consistent use of the / (front slash)

Define context paths on the reverse proxy server exactly the same as paths to a browser URL. For example, if the directive contains a / (front slash) at the end of the mirror path on the reverse proxy server, type / at the end of the browser URL.

You must use a / (front slash) consistently in the source and destination URLs in the directive of the reverse proxy server. That is, if you add a / (front slash) to the end of the source URL, you must also add it to the end of the destination URL.

## 6.19.2 To configure the reverse proxy server

The steps below are required for Information platform services web applications to work behind a supported 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 Information platform services WAR file is required.

3. Configure the reverse proxy server for each Information platform services WAR file. Note that the rules are specified differently on each type of reverse proxy server.
4. Perform any special configuration that is required. Some web applications require special configuration when deployed on certain web application servers.

### 6.19.3 To configure Apache 2.2 reverse proxy server for Information platform services

This section provides a workflow for configuring Information platform services and Apache 2.2 to work together.

1. Ensure that Information platform services and Apache 2.2 are installed on separate computers.
2. Ensure that Apache 2.2 is installed and configured as a reverse proxy server as described in the vendor documentation.
3. Configure the `ProxyPass` for every WAR file that is deployed behind the reverse proxy server.
4. Configure the `ProxyPassReverseCookiePath` for every web application that is deployed behind the reverse proxy server.

### 6.19.4 To configure WebSEAL 6.0 reverse proxy server for Information platform services

This section explains how to configure Information platform services and WebSEAL 6.0 to work together.

The recommended configuration method is to create a single standard junction that maps all of the Information platform services web applications hosted on an internal web application server or web server to a single mount point.

1. Ensure that Information platform services and WebSEAL 6.0 are installed on separate machines.  
It is possible but not recommended to deploy Information platform services 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 `pdadmin sec_master` prompt:

```
server task <instance_name-webseald-host_name>create -t  
<type> -h <host_name> -p <port> <junction_point>
```

Where:

- `<instance_name-webseald-host_name>` specifies the full server name of the installed WebSEAL instance. Use this full server name in the same format as displayed in the output of the `server list` command.
- `<type>` specifies the type of junction. Use `tcp` if the junction maps to an internal HTTP port. Use `ssl` if the junction maps to an internal HTTPS port.
- `<host_name>` specifies the DNS host name or IP address of the internal server that will receive the requests.
- `<port>` specifies the TCP port of the internal server that will receive the requests.
- `<junction_point>` specifies the directory in the WebSEAL protected object space where the document space of the internal server is mounted.

**Example:**

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

---

## 6.19.5 To configure Microsoft ISA 2006 for Information platform services

This section explains how to configure Information platform services and ISA 2006 to work together.

The recommended configuration method is to create a single standard junction that maps all of the Information platform services WAR files hosted on an internal web application server or web server to a single mount point. Depending on your web application server, there are additional configuration required on the application server for it to work with ISA 2006.

1. Ensure that Information platform services and ISA 2006 are installed on separate machines.  
It is possible but not recommended to deploy Information platform services and ISA 2006 on the same machine. Refer to the ISA 2006 documentation for instructions on configuring this deployment scenario.
2. Ensure that ISA 2006 is installed and configured as described in the vendor documentation.
3. Launch the ISA Server Management utility.
4. Use the navigation panel to launch a new publishing rule
  - a. Go to  
**Arrays > MachineName > Firewall Policy > New > Web Site Publishing Rule**
  - Remember:**  
Replace `MachineName` with the name of the machine on which ISA 2006 is installed.
  - b. Type a rule name in **Web publishing rule name** and click **Next**
  - c. Select **Allow** as the rule action and click **Next**.
  - d. Select **Publish a single Web site or load balancer** as the publishing type and click **Next**.
  - e. Select a connection type between the ISA Server and the published Web site and click **Next**.

For example, select **Use non-secured connections to connect the published Web server or server farm**.

- f. Type the internal name of the Web site you are publishing (for example, the machine name hosting Information platform services) in **Internal site name** and click **Next**.

**Note:**

If the machine hosting ISA 2006 cannot connect to the target server select **Use a computer name or IP address to connect to the published server** and type the name or IP address in the field provided.

- g. In "Public Name Details" select the domain name (for example **Any domain name**) and specify any internal publishing details (for example /\*). Click **Next**.

You now need to create a new web listener to monitor for incoming Web requests.

5. Click **New** to launch the New Web Listener Definition Wizard.

- a. Type a name in **Web Listener name** and click **Next**.
- b. Select a connection type between the ISA Server and the published Web site and click **Next**.

For example, select **Do not require SSL secured connections with clients**.

- c. In "Web Listener IP Addresses" section select the following and click **Next**.

- Internal
- External
- Local Host
- All Networks

ISA Server is now configured to publish only over HTTP.

- d. Select an "Authentication Setting" option, click **Next**, and then click **Finish**.

The new listener is now configured for the web publishing rule.

6. Click **Next** in "User Sets", then click **Finish**.

7. Click **Apply** to save all the settings for the web publishing rule and update the ISA 2006 configuration.

You now have to update the properties of the web publishing rule to map paths for the web applications.

8. In the navigation panel, right-click the Firewall Policy you configured and select **Properties**.

9. Select the "Paths" tab and click **Add** to map routes to SAP BusinessObjects web applications.

10. Under "Public Name" tab, select **Request for the following websites** and click **Add**.

11. In the "Public Name" dialog box, type your ISA 2006 server name and click **OK**.

12. Click **Apply** to save all the settings for the web publishing rule and update the ISA 2006 configuration.

13. Verify the connections by accessing the following URL:

`http://<ISA Server host Name>:<web listener port number>/<External path of the application>`

For example: `http://myISAserver:80/Product/BOE/CMC`

**Note:**

You may have to refresh the browser several times.

You need to modify the HTTP policy for the rule you have just configured to ensure that you will be able to logon 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 Information platform services you need to create an access rule.

## 6.20 Special configuration for Information platform services in reverse proxy deployments

Some Information platform services products need additional configuration to function correctly in reverse proxy deployments. This section explains how to perform the additional configuration.

### 6.20.1 Enabling reverse proxy for Information platform services Web Services

This section describes the required procedures to enable reverse proxies for Information platform services Web Services.

#### 6.20.1.1 Enabling reverse proxy for Web Services on web application servers other than Tomcat

The following procedure requires that Information platform services 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.domain.com/dswsbobje/`, update the following properties in the `dsws.properties` file:

- `wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine`
- `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatatalog`
- `wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish`
- `wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService`

- wsresource5=BIPlatform|BIPlatform web service|http://my\_reverse\_proxy\_server.domain.com/SAP/dswsbobje/services/BIPlatform
- wsresource6=LiveOffice|Live Office web service|http://my\_reverse\_proxy\_server.domain.com/SAP/dswsbobje/services/LiveOffice

3. Save and close the `dsws.properties` file.
4. Restart the web application server.
5. Ensure the reverse proxy server maps its virtual path to the correct web application server connector port. The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy Information platform services Web Services deployed on the web application server of your choice:

```
ProxyPass /SAP/dswsbobje http://internalServer:<listening port> /dswsbobje
ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
```

Where `<listening port>` is the listening port of your web application server.

## 6.20.2 Enabling the root path for session cookies for ISA 2006

This section describes how to configure specific web application servers to enable the root path for session cookies to work with ISA 2006 as the reverse proxy server.

### 6.20.2.1 To configure Sun Java 8.2

You need to modify the `sun-web.xml` for every Information platform services web application.

1. Go to `<SUN_WEBAPP_DOMAIN>\generated\xml\j2ee-modules\webapps\BOE\WEB-INF`
2. Open `sun-web.xml`
3. After the `<context-root>` container add the following:

```
<session-config>
  <cookie-properties>
    <property name="cookiePath" value="/" />
  </cookie-properties>
</session-config>
<property name="reuseSessionID" value="true"/>
```

4. Save and close `sun-web.xml`.
5. Repeat steps 1-4 for every web application.

### 6.20.2.2 To configure Oracle Application Server 10gR3

You need to modify the `global-web-application.xml` or `orion-web.xml` for every Information platform services 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.

### 6.20.2.3 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** check box 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.

### 6.20.3 Enabling reverse proxy for SAP BusinessObjects Live Office

To enable SAP BusinessObjects Live Office's View Object in Web Browser feature for reverse proxies, adjust the default viewer URL. This can be done in the Central Management Console (CMC) or through Live Office options.

**Note:**

This section assumes reverse proxies for Information platform services Java BI launch pad and Information platform services Web Services have been successfully enabled.

### **6.20.3.1 To adjust the default viewer URL in the CMC**

1. In the CMC, on the "Applications" page, click **Central Management Console**.
2. Click **Actions > Processing Settings**.
3. In the **URL** box, type the URL for the default viewer, and click **Set URL**.

For example, type `http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?sIDType=CUID&iDocID=%SI_CUID%`, where `ReverseProxyServer` and `ReverseProxyServerPort` are the correct reverse proxy server name and its listen port.

# Authentication

## 7.1 Authentication options in Information platform services

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.

Security plugins expand and customize the ways in which Information platform services authenticates users. Security plugins facilitate account creation and management by allowing you to map user accounts and groups from third-party systems into Information platform services. You can map third-party user accounts or groups to existing Information platform services user accounts or groups, or you can create new Enterprise user accounts or groups that correspond to each mapped entry in the external system.

The current release supports the following authentication methods:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

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

### Related Topics

- [Configuring SAP authentication](#)
- [Enabling JD Edwards EnterpriseOne authentication](#)
- [Enabling Oracle EBS authentication](#)
- [Enabling PeopleSoft Enterprise authentication](#)
- [Enabling Siebel authentication](#)
- [Enterprise authentication overview](#)
- [Using LDAP authentication](#)
- [Using Windows AD authentication](#)

### 7.1.1 Primary authentication

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

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

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

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

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

- The authentication type may be Enterprise, LDAP, Windows AD, SAP, Oracle EBS, Siebel, JD Edwards EnterpriseOne, PeopleSoft Enterprise depending upon which type(s) you have enabled and set up in the Authentication management area of the Central Management Console (CMC). The user's web browser sends the information by HTTP to your web server, which routes the information to the CMS or the appropriate Information platform services server.

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

For instance, if the user is logging on to BI launch pad and specifies Enterprise authentication, the SDK ensures that the Information platform services security plug-in performs the authentication. The Central Management Server (CMS) uses the security plug-in to verify the user name and password against the system database. Alternatively, if the user specifies an authentication method, the SDK uses the corresponding security plug-in to authenticate the user.

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

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

**Note:**

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

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

**Note:**

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

## 7.1.2 Security plug-ins

Security plug-ins expand and customize the ways in which Information platform services authenticates users. Information platform services currently ships with the system default Information platform services security plug-in together with the following plugins:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

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

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

Moreover, security plug-ins enable you to assign rights to users and groups in a consistent manner, because the mapped users and groups are treated as if they were Enterprise accounts. For example, you might map some user accounts or groups from Windows AD, and some from an LDAP directory server. Then, when you need to assign rights or create new, custom groups within Information platform services, 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 Information platform services, they choose from the available authentication types that you have enabled and set up in the Authorization management area of the CMC.

**Note:**

The Windows AD security plugin cannot authenticate users if the Information platform services server components are running on UNIX.

## 7.1.3 Single sign-on to Information platform services

Single sign-on to Information platform services means that once users have logged on to the operating system, they can access Information platform services 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 Information platform services in order to perform SSO - resulting in the user being logged on as an Information platform services user that corresponds to the user.

The term “anonymous single sign-on” also refers to single sign-on to Information platform services , 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 Information platform services as Guest and will have access to Information platform services.

### 7.1.3.1 Single sign-on support

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

Single sign-on to BI launch pad can be provided by Information platform services or by different authentication tools, depending on your application server type and operating system.

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

- Windows AD with Kerberos
- Windows AD with SiteMinder

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

- Windows AD with Kerberos
- Windows AD with NTLM
- Windows AD with SiteMinder

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

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

**Note:**

Windows AD with Kerberos is supported if the Java application is on Unix. However, Information platform services must run on a Windows server.

The following table describes the methods of single sign-on support for BI launch pad.

Authenti- cation Mode	CMS Serv- er	Options	Notes
Windows AD	Windows only	Windows AD with Kerberos only.	Windows AD authentication to BI launch pad and the CMC is available out of the box.
LDAP	Any sup- ported plat- form	Supported LDAP directory servers, with SiteMinder only.	LDAP authentication to BI launch pad and the CMC is available out of the box. SSO to BI launch pad and the CMC requires SiteMinder.
Enterprise	Any sup- ported plat- form	Trusted Authentication	Enterprise authentication to BI launch pad and the CMC is available out of the box. SSO with enterprise authentication to BI launch pad and the CMC requires Trusted Authentication.

**Related Topics**

- [Single sign-on to Information platform services](#)
- [Single sign-on to database](#)
- [End-to-end single sign-on](#)

**7.1.3.2 Single sign-on to database**

Once users are logged on to Information platform services, 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 Information platform services, to provide users with even easier access to the resources they need.

**7.1.3.3 End-to-end single sign-on**

End-to-end single sign-on refers to a configuration where users have both single sign-on access to Information platform services 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 Information platform services and to be able to perform actions that require database access, such as viewing reports.

In Information platform services end-to-end single sign-on is supported through Windows AD and Kerberos.

## 7.2 Enterprise authentication

### 7.2.1 Enterprise authentication overview

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

**Tip:**

Use the system default Enterprise Authentication if you prefer to create distinct accounts and groups for use with Information platform services, or if you have not already set up a hierarchy of users and groups in a third-party directory server.

You do not have to configure or enable Enterprise authentication. You can however modify Enterprise authentication settings to meet your organization's particular security requirements. You can only modify Enterprise setting through the Central Management Console (CMC).

### 7.2.2 Enterprise authentication settings

Settings	Options	Description

Settings	Options	Description
Password Restrictions	<b>Enforce mixed-case password</b>	This option ensures that passwords contain at least two of the following character classes: upper case letters, lower case letters, numbers, or punctuation.
	<b>Must contain at least N characters</b>	By enforcing a minimum complexity for passwords, you decrease a malicious user's chances of simply guessing a valid user's password.
User Restrictions	<b>Must change password every N day(s)</b>	This option ensures that the passwords do not become a liability and are regularly refreshed.
	<b>Cannot reuse the N most recent passwords(s)</b>	This option ensures that passwords will not routinely be repeated.
	<b>Must wait N minute(s) to change password</b>	This option ensures that new passwords cannot be immediately changed once entered into the system.
Logon Restrictions	<b>Disable account after N failed attempts to log on</b>	This security option specifies how many attempts a user is allowed to log on to the system before their account is disabled.
	<b>Reset failed logon count after N minute(s)</b>	This option specifies a time interval for resetting the logon attempt counter.
	<b>Re-enable account after N minute(s)</b>	This option specifies for how long an account is suspended after N failed logon attempts.
Synchronize Data Source Credentials with Log On	<b>Enable and update user's data source credentials at logon time</b>	This option enables data source credentials after the user has logged on.
Trusted Authentication	<b>Trusted Authentication is enabled</b>	This option turns on Trusted Authentication.

### Related Topics

- [Enabling Trusted Authentication](#)

## 7.2.3 To change Enterprise settings

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

2. Double-click **Enterprise**.  
The "Enterprise" dialog box appears.

3. Change the settings.

**Tip:**

To revert all the settings to the default value click **Reset**.

4. Click **Update** to save your modifications.

### 7.2.3.1 To change general password settings

**Note:**

Accounts not used for an extended period of time are not automatically de-activated.

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

Option	Minimum Value	Recommended Maximum Value
<b>Enforce mixed-case passwords</b>	N/A	N/A
<b>Must contain at least N Characters</b>	0 characters	64 characters
<b>Must change password every N day(s)</b>	1 day	100 days
<b>Cannot reuse the N most recent password(s)</b>	1 password	100 passwords
<b>Must wait N minute(s) to change password</b>	0 minutes	100 minutes
<b>Disable account after N failed attempts to log on</b>	1 failed	100 failed

Option	Minimum Value	Recommended Maximum Value
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**.

## 7.2.4 Enabling Trusted Authentication

### Note:

Accounts that are not used for a period of time are not automatically de-activated.

Enterprise Trusted Authentication is used to perform single sign-on by relying on the web application server to verify the identity of a user. This method of authentication involves establishing trust between the Central Management Server (CMS) and the web application server hosting the Information platform services web application. When the trust is established, the system defers the verification of the identity of a user to the web application server. Trusted Authentication can be used to support authentication methods such as SAML, x.509 and other methods which do not have dedicated authentication plugins.

Users prefer to log on to the system once, without needing to provide passwords several times during a session. Trusted Authentication provides a Java single sign-on solution for integrating your Information platform services authentication solution with third-party authentication solutions. Applications that have established trust with the Central Management Server (CMC) can use Trusted Authentication to allow users to log on without providing their passwords.

To enable Trusted Authentication you must configure a shared secret on the server through the Enterprise authentication settings, while the client is configured through the properties specified for the `BOE.war` file.

### 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 Information platform services.
- The single sign-on URL for BI launch pad is `http://server:port/BOE/BI`.

### Related Topics

- [To configure the server to use Trusted Authentication](#)
- [To configure Trusted Authentication for the web application](#)

### 7.2.4.1 To configure the server to use Trusted Authentication

Before you can perform this task, the Enterprise users or mapped third-party users who need to sign on to Information platform services must be created.

You must configure the server and then the client computer for Trusted Authentication.

**Caution:**

Information platform services does not audit modifications to Trusted Authentication parameters. You should manually back up all Trusted Authentication information.

1. On the CMC, go to the **Authentication** management area.
2. Click the **Enterprise** option.  
The "Enterprise" dialog-box appears.
3. Scroll down until you see "Trusted Authentication".
  - a. Click **Trusted Authentication is enabled**.
  - b. Click **New Shared Secret**.  
The shared secret is used by the client computer and the CMS to establish trust.  
The Shared secret key is generated and ready for download message appears.
  - c. Click **Download Shared Secret**.  
The "File Download" dialog box appears.
  - d. Click **Save** and then save the `TrustedPrincipal.conf` file in one of the following directories:
    - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
    - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
  - e. To specify the number of days that your shared secret will be valid, enter a value in the **Shared Secret Validity Period** box.
  - f. Specify the maximum amount of time, in milliseconds, that the clock on the client computer and the clock on the CMS can differ for trusted authentication requests.

**Caution:**

To avoid increasing your vulnerability to replay attacks, do not set this value to 0.

4. Click **Update** to commit the shared secret.

After configuring the server for Trusted Authentication, you must configure the client computer where your app server is located.

### 7.2.5 Configuring Trusted Authentication for the web application

To configure Trusted Authentication for the client, you must modify global properties for the `BOE.war` file and specific properties for BI launch pad and OpenDocument applications.

Use one of the following methods to pass the shared secret to the client:

- `WEB_SESSION` option
- `TrustedPrincipal.conf` file

Use one of the following methods to pass the user name to the client:

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

Regardless of how you pass the shared secret, the method you use must be customized in the `Trusted.auth.user.retrieval` global properties for the `BOE.war` file.

### 7.2.5.1 Using Trusted Authentication for SAML single sign-on

Security Assertion Markup Language (SAML) is an XML-based standard for communicating identity information. SAML provides a secure connection where identity and trust is communicated thereby enabling a single sign-on mechanism that eliminates additional logins for trusted users seeking to access Information platform services.

#### Enabling SAML authentication

If your application server can work as a SAML service provider, you can use Trusted Authentication to provide SAML SSO to the system.

To do this, you must first configure the application server for SAML authentication. Please refer to your application server documentation for further instructions on how to accomplish this, as they will vary by application server.

#### Using Trusted Authentication

Once your web application server is configured to work as a SAML service provider, you can use Trusted Authentication to provide SAML SSO.

#### Note:

Users must either be imported into Information platform services or have Enterprise accounts.

Dynamic aliasing is used to enable the SSO. When a user first accesses the logon page through SAML, they will be asked to manually log in using their existing Information platform services account credentials. Once the user's credentials are verified, the system will alias the user's SAML identity to their Information platform services account. Subsequent logon attempts for the user will be performed using SSO, as the system will have the user's identity alias dynamically matched to an existing account.

**Note:**

A specific property for the BOE.war - `trusted.auth.user.namespace.enabled` - must be enabled for this mechanism to work.

### 7.2.5.2 Trusted Authentication properties for web applications

The following table lists the Trusted Authentication settings included in the default `global.properties` file for BOE.war. To overwrite any settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Property	Default value	Description
<code>sso.enabled=true</code>	<code>sso.enabled=false</code>	Enables and disables single sign-on (SSO) to Information platform services. To enable Trusted authentication, this property must be set to <code>true</code> .
<code>trusted.auth.shared.secret</code>	None	Session variable name used to retrieve the secret for Trusted Authentication. Only applies if using the web session to pass the shared secret.
<code>trusted.auth.user.param</code>	None	Specifies the variable used to retrieve the user name for Trusted Authentication.
<code>trusted.auth.user.retrieval</code>	None	Specifies the method used to retrieve the user name for Trusted Authentication. Can be set to one of the following: <ul style="list-style-type: none"> <li>"REMOTE_USER"</li> <li>"HTTP_HEADER"</li> <li>"COOKIE"</li> <li>"QUERY_STRING"</li> <li>"WEB_SESSION"</li> <li>"USER_PRINCIPAL"</li> </ul> If the property is blank, Trusted Authentication is disabled.
<code>trusted.auth.user.namespace.enabled</code>	None	Enables and disables dynamic binding of aliases to existing user accounts. If the property is set to <code>true</code> , Trusted Authentication uses alias binding to authenticate users to Information platform services. With alias binding, your application server can work as a SAML service provider, enabling Trusted Authentication to provide SAML single sign-on to the system. If the property is blank, Trusted Authentication will use name matching when authenticating users.

### 7.2.5.3 To configure Trusted Authentication for the web application

If you plan to store the shared secret in the `TrustedPrincipal.conf` file, make sure the file is located in the appropriate platform directory:

Platform	Location of TrustedPrincipal.conf
Windows, default installation	<ul style="list-style-type: none"> <li>• &lt;INSTALLDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\win32_x86\</li> <li>• &lt;INSTALLDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64\</li> </ul>
AIX	<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000/
Solaris	<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparc/
HP_UX	<INSTALLDIR>/sap_bobj/enterprise_xi40/hpux_pa-risc/
Linux	<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86

Various mechanisms populate the user name variable that is used to configure Trusted Authentication for the client hosting web applications. Configure or set up your web application server so that your user names are exposed before you use the user retrieval name methods. See <http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html> for further information.

To configure Trusted Authentication for the client, you must access and modify properties for the `BOE.war` file, which includes general and specific properties for BI launch pad and OpenDocument web applications.

**Note:**

Additional steps may be required, depending on how you plan to retrieve the user name or shared secret.

1. Access the custom folder for the `BOE.war` file on the machine hosting the web applications.

If you are using the Tomcat web application server provided with the Information platform services installation, you can access the following folder:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
```

**Tip:**

If you are using a web application server that does not enable direct access to the deployed web applications, use the following folder in your product installation to modify the `BOE.war` file:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

Later, you must redeploy the modified `BOE.war` file.

2. Create a new file, using Notepad or another text editing utility.
3. Enter the following trusted authentication properties:

```
sso.enabled=true
trusted.auth.user.retrieval=Method for user ID retrieval
trusted.auth.user.param=Variable
trusted.auth.shared.secret=WEB_SESSION
```

For the `trusted.auth.shared.secret` property, select one of the following options for user name retrieval:

Option	How the user name will be retrieved
HTTP_HEADER	The user name is retrieved from the contents of an HTTP header. You specify which HTTP header to use in the <code>trusted.auth.user.param</code> property.
QUERY_STRING	The user name is retrieved from a parameter of the request URL. You specify which query string to use in the <code>trusted.auth.user.param</code> property.
COOKIE	The user name is retrieved from a specified cookie. You specify which cookie to use in the <code>trusted.auth.user.param</code> property.
WEB_SESSION	The user name is retrieved from the contents of a specified session variable. You specify the web session variable to use in the <code>trusted.auth.user.param</code> property in <code>global.properties</code> .
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.
REMOTE_USER	The user name is retrieved from a call to <code>HttpServletRequest.getRemoteUser()</code> .

**Note:**

- Some web application servers require the environment variable `REMOTE_USER` set to `true` on the server. To find out whether this is required, see your web application server documentation. If it is required, confirm that the environment variable is set to `true`.
- If you are using `USER_PRINCIPAL` or `REMOTE_USER` to pass the user name, leave the `trusted.auth.user.param` blank.

4. Save the file with the name `global.properties`.

5. Restart your web application server.

The new properties take effect only after the modified BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy, see the *Information platform services Web Application Deployment Guide*.

### 7.2.5.3.1 Sample configurations

#### *To pass the shared secret through the TrustedPrincipal.conf file*

The following sample configuration assumes that a user *JohnDoe* has been created in Information platform services.

The user information will be stored and passed through the web session, while the shared secret will be passed via the `TrustedPrincipal.conf` file. This file is assumed to be in the following directory: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. The bundled version of Tomcat 6 is the web application server.

1. In the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory, use Notepad or another text editing utility to create a new file.
2. In the new file, enter the following Trusted Authentication properties:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

3. Save the file with the name `global.properties`.
4. Locate the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp` file.
5. In the `custom.jsp` file, enter the following properties:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:gotoLogonPage()">Click this to go to the logon page of BI launch pad</a>
```

```
</body>
</html>
```

6. Create a `myScript.js` file in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCus tomResources` directory.
7. In the `myScript.js` file, enter the following properties:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

8. Stop the Tomcat server.
9. Delete the `work` folder in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6` directory.
10. Restart Tomcat.

To verify that you have properly configured Trusted Authentication, go to `http://[cmsname]:8080/BOE/BI/custom.jsp` to access BI launch pad, where `[cmsname]` is the name of the computer hosting the CMS. The following link should appear: **Click this to go to the logon page of BI launch pad**

### *To pass the shared secret through the web session variable*

The following sample configuration assumes that a user `JohnDoe` has been created in Information platform services.

User information is stored and passed via the web session, and the shared secret is passed via the web session variable, which is located by default in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` directory. You need to open and note the content of the file. In this sample configuration, the shared secret is:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

The bundled version of Tomcat 6 is the web application server.

1. In the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory, use Notepad or another text editing utility to create a new file.
2. In the new file, enter the following Trusted Authentication properties:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

3. Save the file with the name `global.properties`.
4. Locate the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp` file.
5. In the `custom.jsp` file, enter the following properties:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
```

```
//custom Java code
request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db82112934
86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345
285b55a0a7"
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI launch pad</a>
</body>
</html>
```

6. Create a `myScript.js` file in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources` directory.
7. In the `myScript.js` file, enter the following properties:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

8. Stop the Tomcat server.
9. Delete the work folder in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6` directory.
10. Restart Tomcat.

To verify that you have properly configured Trusted authentication, use the following URL to access the BI launch pad application: `http://[cmsname]:8080/BOE/BI/custom.jsp`, where `[cmsname]` is the name of the computer hosting the CMS. The following link should appear: **Click this to go to the logon page of BI launch pad**

### *To pass the user name through user principal*

The following sample configuration assumes that a user called *JohnDoe* has been created in Information platform services.

User information is stored and passed through the **User Principal** option, and the shared secret is passed via the `TrustedPrincipal.conf` file, which is located by default in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` directory. The bundled version of Tomcat 6 is the web application server.

#### **Note:**

The web application server configuration is the same for the `USER_PRINCIPAL` method and the `REMOTE_USER` method.

1. Stop the Tomcat server.
2. Open the `server.xml` file for Tomcat in the default `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\conf` directory.
3. Locate the `<Realm className="org.apache.catalina.realm.UserDatabaseRealm".../>` tag, and change it to the following value:
 

```
<Realm className="org.apache.catalina.realm.MemoryRealm".../>
```

4. Open the `tomcat-users.xml` file in the default `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\conf` directory.
5. Locate the `<tomcat-users>` tag, and enter the following values:

```
<user name="JohnDoe" password="password"
roles="onjavauser"/>
```

6. Open the `web.xml` file in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF` directory.
7. Before the `</web-app>` tag, insert the following tags:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>OnJavaApplication</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>onjavauser</role-name>
  </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>OnJava Application</realm-name>
</login-config>
```

**Note:**

You must add a page for the `<url-pattern></url-pattern>` tag. Typically this page is not the default URL for BI launch pad or any other web application.

8. Open the custom `global.properties` file, and enter the following values:
  - `trusted.auth.user.retrieval=USER_PRINCIPAL`
  - (Optional) `trusted.auth.user.namespace.enabled=true` to map an external user name to a different BOE user name
9. Delete the `work` folder in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6` directory.
10. Restart Tomcat.

To verify that you have properly configured Trusted authentication, go to `http://[cmsname]:8080/BOE/BI` to access BI launch pad, where `[cmsname]` is the name of the computer hosting the CMS. After a few moments a logon dialog box appears.

## 7.3 LDAP authentication

### 7.3.1 Using LDAP authentication

This section provides a general description of how LDAP authentication works with Information platform services. It then introduces the administration tools that allow you to manage and configure LDAP accounts to Information platform services.

When you install Information platform services, the LDAP authentication plug-in is installed automatically, but not enabled by default. To use LDAP authentication, you need to first ensure that you have your respective LDAP directory set up. For more information about LDAP, refer to your LDAP documentation.

Lightweight Directory Access Protocol (LDAP), a common, application-independent directory, enables users to share information among various applications. Based on an open standard, LDAP provides a means for accessing and updating information in a directory.

LDAP is based on the X.500 standard, which uses a directory access protocol (DAP) to communicate between a directory client and a directory server. LDAP is an alternative to DAP because it uses fewer resources and simplifies and omits some X.500 operations and features.

The directory structure within LDAP has entries arranged in a specific schema. Each entry is identified by its corresponding distinguished name (DN) or common name (CN). Other common attributes include the organizational unit name (OU), and the organization name (O). For example, a member group may be located in a directory tree as follows: cn=Information platform services 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 Information platform services through LDAP authentication. It also enables users to be authorized when attempting to access objects in Information platform services. As long as you have an LDAP server (or servers) running, and use LDAP in your existing networked computer systems, you can use LDAP authentication (along with Enterprise, and Windows AD authentication).

If desired, the LDAP security plug-in provided with Information platform services 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 Information platform services 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 Information platform services 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 Information platform services 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 Information platform services, ensure that you are familiar with the differences between these LDAP types. For details, see RFC2251, which is currently available at <http://www.faqs.org/rfcs/rfc2251.html>.

### **Related Topics**

- [Configuring LDAP authentication](#)
- [Mapping LDAP groups](#)

### 7.3.1.1 LDAP security plugin

The LDAP security plug-in allows you to map user accounts and groups from your LDAP directory server to Information platform services; 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 Information platform services session. User lists and group memberships are dynamically maintained by Information platform services. You can specify that Information platform services use a Secure Sockets Layer (SSL) connection to communicate to the LDAP directory server for additional security.

LDAP authentication for Information platform services is similar Windows 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.
- Specify multiple host names and their ports.
- Configure LDAP with SiteMinder.

Once you have mapped your LDAP users and groups, all of the Information platform services client tools support LDAP authentication. You can also create your own applications that support LDAP authentication.

#### **Related Topics**

- [Configuring SSL settings for LDAP Server or Mutual Authentication](#)
- [Configuring the LDAP plug-in for SiteMinder](#)

## 7.3.2 Configuring LDAP authentication

To simplify administration, Information platform services supports LDAP authentication for user and group accounts. Before users can use their LDAP user name and password to log on to Information platform services, you need to map their LDAP account to Information platform services. When you map an LDAP account, you can choose to create a new account or link to an existing Information platform services account.

Before setting up and enabling LDAP authentication, ensure that you have your LDAP directory set up. For more information, refer to your LDAP documentation.

Configuring LDAP authentication includes the following tasks:

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

**Note:**

If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.

### 7.3.2.1 To configure the LDAP host

Before configuring the LDAP host, your LDAP server must be installed and running.

1. In the "Authentication" management area of the CMC, double-click **LDAP**.

**Tip:**

To go to the "Authentication" management area, click **Authentication** in the navigation list.

2. Type the name and port number of your LDAP hosts in the **Add LDAP host (hostname:port)** box (for example, myserver:123), click **Add**, and 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. To remove a host, select the host name and click **Delete**.

3. In the **LDAP Server Type** list, select your server type.

**Note:**

If you are mapping LDAP to AD, select **Microsoft Active Directory Application Server** for your server type.

4. To view or change **LDAP Server Attribute Mappings** or **LDAP Default Search Attributes**, click **Show Attribute Mappings**.

By default, each supported server type's server attribute mappings and search attributes are already set.

5. Click **Next**.

6. In the **Base LDAP Distinguished Name** box, type a distinguished name (for example, o=SomeBase) for your LDAP server, and click **Next**.

7. In the "LDAP Server Credentials" area, type a 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. Information platform services servers and client computers will bind to the primary host via anonymous logon.

8. If you configured referrals on your LDAP host, enter authentication information under "LDAP Referral Credentials", and type the number of referral hops in the **Maximum Referral Hops** box.

**Note:**

You must configure the "LDAP Referral Credentials" area if all of the following conditions apply:

- The primary host is configured to refer to another directory server that handles queries for entries under a specified base.
- The host being referred to is configured to not allow anonymous binding.
- A group from the host being referred to will be mapped to Information platform services.

**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 0 (zero), no referrals will be followed.
9. Click **Next**, and choose the type of Secure Sockets Layer (SSL) authentication used:
    - **Basic (no SSL)**
    - **Server Authentication**
    - **Mutual Authentication**
  10. Click **Next**, and choose **Basic (No SSO)** or **SiteMinder** as the method of LDAP single sign-on authentication.
  11. Click **Next**, and select how aliases and users are mapped to Information platform services accounts:
    - a. In the **New Alias Options** list, select an option for mapping new aliases to Enterprise accounts:
      - **Assign each added LDAP alias to an account with the same name**

Use this option when you know users have an existing Enterprise account with the same name; that is, LDAP aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account or who do not have the same name in their Enterprise and LDAP account are added as new users.
      - **Create a new account for every added LDAP alias**

Use this option when you want to create a new account for each user.
    - b. In the **Alias Update Options** list, select an option for managing alias updates for Enterprise accounts:
      - **Create new aliases when the Alias Update occurs**

Use this option to automatically create a new alias for every LDAP user mapped to Information platform services. New LDAP accounts are added for users without Information platform services accounts or for all users if you selected **Create a new account for every added LDAP alias**.

- **Create new aliases only when the user logs on**

Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use Information platform services. The system does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to Information platform services.
  - c. If your Information platform services license is based on users roles, in the **New User Options** list, select an option to specify how new users are created:
    - **BI Viewer**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.
    - **BI Analyst**

New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all application workflows that are defined for the BI Analyst role. Access rights include viewing and modifying Business Intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.
  - d. If your Information platform services license is not based on users roles, in the **New User Options** list, select an option to specify how new users are created:
    - **New users are created as named users**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.
    - **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 Information platform services 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 Information platform services, a 100-user concurrent license could support 250, 500, or 700 users.
12. Under "Attribute Binding Options", specify the attribute binding priority for the LDAP plugin:
- a. Click the **Import Full Name, Email Address and other attributes** box.

The full names and descriptions used in the LDAP accounts are imported and stored with the user objects in Information platform services.
  - b. Specify an option for **Set priority of LDAP attribute binding relative to other attributes binding**.

**Note:**

If option is set to **1**, LDAP attributes take priority in scenarios where LDAP and other plugins (Windows AD and SAP) are enabled. If it is set to **3**, attributes from other enabled plugins take priority.

13. Click **Finish**.

**Related Topics**

- [Configuring SSL settings for LDAP Server or Mutual Authentication](#)
- [Configuring the LDAP plug-in for SiteMinder](#)
- [Role-based licensing](#)

### 7.3.2.2 Managing multiple LDAP hosts

Using LDAP and Information platform services, you can add fault tolerance to your system by adding multiple LDAP hosts. Information platform services uses the first host that you add as the primary LDAP host. Subsequent hosts are treated as failover hosts.

The primary LDAP host and all failover hosts must be configured in exactly the same way, and each LDAP host must refer to all additional hosts from which you want to map groups. For more information about LDAP hosts and referrals, see your LDAP documentation.

To add multiple LDAP Hosts, enter all hosts when you configure LDAP using the LDAP configuration wizard (see for details.) Or if you have already configured LDAP, go to the Authentication management area of the Central Management Console and click the LDAP tab. In the LDAP Server Configuration Summary area, click the name of the LDAP host to open the page that enables you to add or delete hosts.

**Note:**

- Make sure that you add the primary host first, followed by the remaining failover hosts.
- If you use failover LDAP hosts, you cannot use the highest level of SSL security (that is, you cannot select "Accept server certificate if it comes from a trusted Certificate Authority and the CN attribute of the certificate matches the DNS hostname of the server.")

**Related Topics**

- [Configuring LDAP authentication](#)

### 7.3.2.3 Configuring SSL settings for LDAP Server or Mutual Authentication

This section describes the CMC related information for configuring SSL with LDAP Server and Mutual Authentication. It assumes that you have configured the LDAP host and that you selected either of these for your SSL authentication choice:

- Server Authentication
- Mutual Authentication

For additional information or for information on configuring the LDAP host server, refer to your LDAP vendor documentation.

**Related Topics**

- [To configure the LDAP host](#)

## 7.3.2.3.1 To configure the LDAP Server or Mutual Authentication

Resource	Take this action before starting this task
CA certificate	<p>This action is required for both server and Mutual Authentication with SSL.</p> <ol style="list-style-type: none"> <li>1. Obtain a Certificate Authority (CA) to generate a CA certificate.</li> <li>2. Add the certificate to your LDAP Server.</li> </ol> <p>For information, see your LDAP vendor documentation.</p>
Server certificate	<p>This action is required for both server and Mutual Authentication with SSL.</p> <ol style="list-style-type: none"> <li>1. Request and then generate a server certificate.</li> <li>2. Authorize the certificate and then add it to the LDAP Server.</li> </ol>
cert7.db, cert8.db, key3.db	<p>These files are required for both server and Mutual Authentication with SSL.</p> <ol style="list-style-type: none"> <li>1. Download the certutil application that generates either a cert7.db or cert8.db file (depending on your requirements) from <a href="ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/">ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/</a>.</li> <li>2. Copy the CA certificate to the same directory as the certutil application.</li> <li>3. Use the following command to generate the cert7.db or cert8.db, key3.db, and secmod.db files: <pre>certutil -N -d .</pre> </li> <li>4. Use the following command to add the CA certificate to the cert7.db or cert8.db file: <pre>certutil -A -n &lt;CA_alias_name&gt; -t CT -d . -I cacert.cer</pre> </li> <li>5. Store the three files in a directory on the computer that hosts Information platform services.</li> </ol>
cacerts	<p>This file is required for server or Mutual Authentication with SSL for Java applications, like BI launch pad.</p> <ol style="list-style-type: none"> <li>1. Locate the keytool file in your Java bin directory.</li> <li>2. Use the following command to create the cacerts file: <pre>keytool -import -v -alias &lt;CA_alias_name&gt; -file &lt;CA_certificate_name&gt; -trustcacerts -keystore</pre> </li> <li>3. Store the cacerts file in the same directory as the cert7.db or cert8.db and key3.db files.</li> </ol>
Client certificate	

Resource	Take this action before starting this task
	<ol style="list-style-type: none"> <li>1. Create separate client requests for the <code>cert7.db</code> or <code>cert8.db</code> and <code>.keystore</code> files: <ul style="list-style-type: none"> <li>• To configure the LDAP plugin, use the <code>certutil</code> application to generate a client certificate request.</li> <li>• Use the following command to generate the client certificate request: <pre>certutil -R -s "&lt;client_dn&gt;" -a -o &lt;certificate_request_name&gt; -d .</pre> <p><code>&lt;client_dn&gt;</code> includes information such as "CN=<code>&lt;client_name&gt;</code>, OU=<code>org unit</code>, O=<code>Companyname</code>, L=<code>city</code>, ST=<code>province</code>, and C=<code>country</code>.</p> </li> </ul> </li> <li>2. Use the CA to authenticate the certificate request. Use the following command to retrieve the certificate and insert it in the <code>cert7.db</code> or <code>cert8.db</code> file: <pre>certutil -A -n &lt;client_name&gt; -t Pu -d . -I &lt;client_certificate_name&gt;</pre> </li> <li>3. To facilitate Java authentication with SSL: <ul style="list-style-type: none"> <li>• Use the <code>keytool</code> utility in the Java <code>bin</code> directory to generate a client certificate request.</li> <li>• Use the following command to generate a key pair: <pre>keytool -genkey -keystore .keystore</pre> </li> </ul> </li> <li>4. After specifying information about your client, use the following command to generate a client certificate request: <pre>keytool -certreq -file &lt;certificate_request_name&gt; -keystore .keystore</pre> </li> <li>5. After the client certificate request is authenticated by the CA, use the following command to add the CA certificate to the <code>.keystore</code> file: <pre>keytool -import -v -alias &lt;CA_alias_name&gt; -file &lt;ca_certificate_name&gt; -trustcacerts -keystore .keystore</pre> </li> <li>6. Retrieve the client certificate request from the CA, and use the following command to add it to the <code>.keystore</code> file: <pre>keytool -import -v -file &lt;client_certificate_name&gt; -trustcacerts -keystore .keystore</pre> </li> <li>7. Store the <code>.keystore</code> file in the same directory as the <code>cert7.db</code> or <code>cert8.db</code> and <code>cacerts</code> files on the computer that hosts Information platform services.</li> </ol>

1. Choose the level of SSL security to use:

- **Always accept server certificate**

This is the lowest security option. Before Information platform services 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. Information platform services 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 Information platform services 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, Information platform services must find the CA that issued the certificate in its certificate database.

- **Accept server certificate if it comes from a trusted Certificate Authority and the CN attribute of the certificate matches the DNS hostname of the server**

This is the highest security option. Before Information platform services 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, Information platform services must find the CA 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 LDAP host name you entered in the **Add LDAP host** box in the first step of the wizard—if you entered the LDAP host name as ABALONE.rd.crystald.net:389. (Using CN =ABALONE:389 in the certificate doesn't work.)

The host name on the server security certificate is the name of the primary LDAP host. Therefore if you select this option you cannot use a failover LDAP host.

**Note:**

Java applications ignore the first and last setting and accept the server certificate only if it comes from a trusted CA.

2. In the **SSL host** box, type the host name of each computer, and click **Add**.

Next, you must add the host name of each computer in your Information platform services system that uses the Information platform services SDK. (This includes the computer running your Central Management Server and the computer running your web application server.)

3. Specify the SSL settings for each SSL host you added to the list:

- a. Select **default** in the SSL list.
- b. Clear the **Use default value** check boxes.
- c. Type a value in the **Path to the certificate and key database files** box and the **Password for the key database** box.
- d. If specifying settings for mutual authentication, type a value in the **Nickname for the client certificate in the cert7.db** box or the **Nickname for the client certificate in the cert8.db** box.

**Note:**

The default settings will be used (for any setting) for any host with the **Use default value** check box selected or for any computer name you do not add to the list of SSL hosts.

4. Specify the default settings for each host that isn't in the list, and click **Next**.

To specify settings for another host, select the host name in the list on the left, and type values in the boxes on the right.

**Note:**

The default settings will be used for any setting (for any host) with the **Use default value** check box selected or for any computer name you do not add to the list of SSL hosts.

5. Select **Basic (No SSO)** or **SiteMinder** as the method of LDAP single sign-on authentication.
6. Choose how new LDAP users and aliases are created.
7. Click **Finish**.

**Related Topics**

- [Configuring the LDAP plug-in for SiteMinder](#)

### 7.3.2.4 To modify your LDAP configuration settings

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.

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 are no longer accessible under the new connection settings, and click **Update**.
4. Change your connection settings, then click **Update**.
5. Change your "Alias and New User" options, and click **Update**.
6. Map your new LDAP member groups, and click **Update**.

### 7.3.2.5 Configuring the LDAP plug-in for SiteMinder

This section explains how to configure the CMC to use LDAP with SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the LDAP security plug-in to create single sign-on to Information platform services.

To use SiteMinder and LDAP with Information platform services, you must make configuration changes in the following two places:

- LDAP plugin through the CMC

- BOE.war file properties

**Note:**

Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done regardless of what supported version of SiteMinder you are using. For more information about SiteMinder and how to install it, see the SiteMinder documentation.

**Related Topics**

- [To configure the LDAP host](#)

### 7.3.2.5.1 To configure LDAP for single sign-on with SiteMinder

1. Open the **Please configure your SiteMinder settings** screen using one of the following methods:
  - Select SiteMinder on the "Please choose a method of LDAP single sign-on authentication" screen in the LDAP configuration wizard.
  - Select 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.
5. Click **Next**.
6. Proceed with configuring the LDAP options.

### 7.3.2.5.2 To enable LDAP and SiteMinder in the BOE.war file

In addition to specifying SiteMinder settings for the LDAP security plugin, SiteMinder settings must be specified for the BOE.war properties.

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

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Create a new file using Notepad or another text editing utility.
3. Enter the following statement:

```
siteminder.authentication=secLDAP  
siteminder.enabled=true
```

4. Close the file and save it under the following name:

```
global.properties
```

**Note:**

Make sure the file name is not saved under any extensions such as `.txt`.

5. Create another file in the same directory.
6. Enter the following statement:

```
authentication.default=LDAP  
cms.default=[enter your cms name]:[Enter the CMS port number]
```

For example:

```
authentication.default=LDAP  
cms.default=mycms:6400
```

7. Close the file and save it under the following name:

```
bilaunchpad.properties
```

The new properties take effect only after the modified BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy, see the *Information platform services Web Application Deployment Guide*.

### 7.3.3 Mapping LDAP groups

Once you have configured the LDAP host using the LDAP configuration wizard, you can map LDAP groups to Enterprise groups.

Once you have mapped LDAP groups, you can view the groups by clicking the LDAP option in the **Authentication** management area. If LDAP authorization is configured, the Mapped LDAP Member Groups area displays the LDAP groups that have been mapped to Information platform services.

You can also map Windows AD groups to authenticate in Information platform services via the LDAP security plugin.

**Note:**

If you have configured LDAP against AD, this procedure will map your AD groups.

**Related Topics**

- [Mapping LDAP against Windows AD](#)

#### 7.3.3.1 To map LDAP groups using Information platform services

1. In the "Authentication" management area of the CMC, double-click **LDAP**.  
If LDAP authorization is configured, the LDAP summary page appears.
2. Under "Mapped LDAP Member Groups", enter your LDAP group (by common name or distinguished name) in the **Add LDAP group (by cn or dn)** box, and click **Add**.

To add more than one LDAP group, repeat this step. To remove a group, select the LDAP group, and click **Delete**.

3. Under "New Alias Options", select an option to specify how LDAP aliases are mapped to Enterprise accounts:

- **Assign each added LDAP alias to an account with the same name**

Use this option when you know users have an existing Enterprise account with the same name; that is, LDAP aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and LDAP account, are added as new LDAP users.

- **Create a new account for every added LDAP alias**

Use this option when you want to create a new account for each user.

4. Under "Alias Update Options", select one of the following options to specify whether LDAP aliases are automatically created for all new users:

- **Create new aliases when the Alias Update occurs**

Use this option to automatically create a new alias for every LDAP user mapped to Information platform services. New LDAP accounts are added for users without Information platform services accounts or for all users, if you selected the **Create a new account for every added LDAP alias** option and clicked **Update**.

- **Create new aliases only when the user logs on**

Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use Information platform services. Information platform services 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 Information platform services.

5. Under "New User Options", specify properties for the new Enterprise accounts created to map to LDAP accounts.

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

- **BI Viewer User**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.

- **BI Analyst User**

New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all application workflows that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.

If your Information platform services license is not based on users roles, select one of the following options:

- **New users are created as named users**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

- **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 Information platform services 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 Information platform services, a 100-user concurrent license could support 250, 500, or 700 users.

6. Click **Update**.

#### **Related Topics**

- [Role-based licensing](#)

### **7.3.3.2 To unmap LDAP groups using Information platform services**

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 Information platform services.

#### **Note:**

The only exceptions to this occur when a user has an alias to an Enterprise account. To restrict access, disable or delete the user's Enterprise account.

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

### **7.3.3.3 Mapping LDAP against Windows AD**

If you configure LDAP against Windows ADauthen, 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 Information platform services 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"> <li>• universal groups on a child domain,</li> <li>• groups on the same domain that contains universal groups from a child domain, and</li> <li>• universal groups on a cross domain.</li> </ul> <p>You cannot map in:</p> <ul style="list-style-type: none"> <li>• global groups on a child domain,</li> <li>• local groups on a child domain,</li> <li>• groups on the same domain that contain a global group from the child domain, and</li> <li>• cross-domain global groups.</li> </ul> <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	To map in universal groups, you must point to the Global Catalog Domain Controller. You should also use port number 3268 instead of the default 389.

- If you are using multiple domains but not pointing to the Global Catalog Domain Controller, then you cannot map in any type of groups from cross or child domains. You can map in all types of groups only from the specific domain you are pointing to.

### **7.3.3.4 Troubleshooting LDAP accounts**

- If you create a new LDAP user account—and the account does not belong to a group account that is mapped to Information platform services—map the group to Information platform services or add the new LDAP user account to a group that is already mapped to Information platform services.
- If you create a new LDAP user account—and the account belongs to a group account that is mapped to Information platform services—refresh the user list.

#### **Related Topics**

- [Configuring LDAP authentication](#)
- [Mapping LDAP groups](#)

## **7.4 Windows AD authentication**

### **7.4.1 Overview**

#### **7.4.1.1 Using Windows AD authentication**

This section provides a general description of how Windows Active Directory (AD) authentication works with Information platform services. It then introduces the administration workflows required to enable and manage AD accounts in Information platform services. At the end of the section, there are some basic troubleshooting tips.

### **Support requirements**

To facilitate AD authentication on Information platform services, you should remember the following support requirements.

- The CMS must always be installed on a supported Windows platform.
- Although Windows 2003 and 2008 are supported platforms for both Kerberos and NTLM authentication, certain Information platform services applications may only use particular authentication methods. For example, applications such as Information platform services BI launch pad and Information platform services Central Management Console only support Kerberos.

### **Basic AD authentication workflow**

To use AD authentication with Information platform services you must follow the following basic workflow:

1. Configure the required domain controller resources.
2. Prepare the Information platform services host for Windows AD authentication.
3. Enable the AD security plug-in and map in AD groups.
4. Choose an authentication method:
  - Windows AD with Kerberos
  - Windows AD with NTLM
5. Set up single sign-on to Information platform services applications. This optional step can be facilitated via the following methods:
  - Windows AD with Vintela (Kerberos)
  - Windows AD with SiteMinder (Kerberos)

#### **7.4.1.1.1 Windows AD security plug-in**

The Windows AD security plug-in enables you to map user accounts and groups from your Microsoft Active Directory (AD) 2003, and 2008 user database to Information platform services. It also enables Information platform services to verify all logon requests that specify AD Authentication. Users are authenticated against the AD user database, and have their membership in a mapped AD group verified before the Central Management Server (CMS) grants them an active Information platform services session.

The Windows AD security plug-in enables you to configure the following:

- Windows AD authentication with NTLM
- Windows AD authentication with Kerberos
- Windows AD authentication with SiteMinder for single sign-on

The Windows AD security plug-in is compatible with both Microsoft Active Directory 2003, and 2008 domains running in either native mode or mixed mode.

Once you have mapped your AD users and groups, all of the Information platform services client tools support AD authentication.

- Windows 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 Information platform services supports domains within multiple forests.

#### 7.4.1.1.2 Using Windows AD users and groups

Information platform services supports Active Directory (AD) authentication with the Windows security plug-in, which is included by default when the product is installed on a Windows platform. Support for Windows AD authentication means that users and groups accounts in Microsoft Active Directory (2003 and 2008) can be used to authenticate with Information platform services. System administrator can therefore map existing AD accounts, instead of setting up each user and group within Information platform services.

#### *Scheduling updates for Windows AD groups*

Information platform services enables administrators to schedule updates for Windows AD groups and user aliases. This feature is available for AD authentication with either Kerberos or NTLM. The CMC also enables you to view the time and date when the last update was performed.

#### **Note:**

For AD authentication to work on Information platform services, you must configure how updates are scheduled for your AD groups and aliases.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can specify what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.

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 a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will be run on the dates specified in a calendar that has previously been created.

### Scheduling AD group updates

Information platform services relies on Active Directory (AD) for user and group information. To minimize the volume of queries sent to AD, the AD plugin caches information about groups and how they relate to each other and their user membership. The update does not run when no specific schedule is defined.

You must use the CMC to configure the recurrence of the group update refresh. This should be scheduled to reflect how frequently your will group membership information is modified.

### 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 Information platform services. Updates to AD accounts are propagated to Information platform services by the AD plug-in. Accounts created, deleted, or disabled in AD will be correspondingly created, deleted, or disabled in Information platform services.

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 Groups and Aliases now** option from the "On-Demand AD Update" area of the CMC.

#### Note:

No AD passwords are stored in the user alias.

#### 7.4.1.1.3 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 Information platform services without explicitly entering their credentials. The single sign-on requirements depend upon the way in which users access Information platform services: 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 Information platform services session if the user is a member of a mapped AD group.

The most common usage scenario involves single sign-on to the BI launch pad web application.

### **Single sign-on to database**

The Windows AD plug-in supports single sign-on to database. If set properly authenticated AD users do not have to provide their account credentials when accessing reports from the BI launch pad application.

## **7.4.2 Preparing for AD authentication (Kerberos)**

### **7.4.2.1 Using Kerberos authentication for Windows AD**

This section describes the prerequisite tasks required for setting up the Kerberos authentication for Information platform services. Once all the prerequisite tasks have been implemented, you can proceed to configure Windows AD authentication options for Kerberos in the Windows AD security plug-in.

#### **Recommended workflow**

To properly set up Windows AD authentication the following prerequisite tasks need to be implemented:

- Setting up a service account for running Information platform services
- Preparing the Information platform services servers for Windows AD authentication with Kerberos
- Configuring your web application server for Windows AD authentication with Kerberos.

#### **7.4.2.1.1 Setting up a service account for AD authentication with Kerberos**

To configure Information platform services 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 Information platform services servers.

#### **Note:**

After you set up the service account, you will need to grant the account appropriate rights.

If you are using a Windows 2003 or 2008 Domain, you also have the option of setting up constrained delegation.

#### *To set up the service account on a Windows 2003 or 2008 domain*

You need to set up a new service account on the domain controller to successfully enable Windows AD authentication with Kerberos. This task is performed on the AD domain controller machine.

1. Create a new account with a password on the domain controller or use an existing account.

For detailed instructions, refer to "<http://msdn.microsoft.com/> "

2. Run the keytab `ktpass` command to create and place a Kerberos keytab file.

You will need to specify the `ktpass` parameters listed in the following table:

Parameter	Description
<code>-out</code>	Specifies the name of the Kerberos keytab file to generate.
<code>-mapuser</code>	Specifies the name of the user account to which the SPN mapped. This is account under which the server intelligence agent runs.
<code>-pass</code>	Specifies the password used by the service account.
<code>-ptype</code>	Specifies the principal type. Should be specified as: <pre>-ptype KRB5_NT_PRINCIPAL</pre>
<code>-crypto</code>	Specifies which encryption type to use with the service account. Use the following: <pre>-crypto RC4-HMAC-NT</pre>

For example,

```
ktpass -out -mapuser sbo.serviceDOMAIN.COM -pass password
-kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

The output from the `ktpass` command should confirm the target domain controller, and that a Kerberos keytab file containing the shared secret has been created. The command also maps the principal name to the (local) service account.

3. Run the `setspn -l` command to verify that the `ktpass` command was successfully executed. The display output lists all the service principal names registered to the local service account.
4. Right-click the service account you created in Step 1, select **Properties > Delegation**.
5. Click **Trust this user for delegation to any service (Kerberos only)**.
6. Click **OK** to save your settings.

Once created, the service account needs to be granted rights and added to the servers's Local Administrators group.

### *Granting the service account rights*

To support Windows 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 Central Management Server (CMS).

If you require single sign-on to the database, the SIA must include the following servers:

- Crystal Reports Processing Server
- Report Application Server
- Web Intelligence Processing Server

**Note:**

For single sign-on to the database to work, the service account must be trusted for delegation.

*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 Information platform services 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. 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 Information platform services server that has to be configured.

#### 7.4.2.1.2 Preparing the servers for Windows AD authentication with Kerberos

After the service account has been created and configured for Windows AD authentication with Kerberos, you can run each SIA in your Information platform services deployment under the account.

##### *To configure the SIA under the service account*

Perform the following steps for any Server Intelligence Agent (SIA) that is running services used by the service account created for Windows AD authentication with Kerberos.

1. To start the CCM, choose **Programs > SAP BusinessObjects BI platform 4 > SAP BusinessObjects BI platform > Central Configuration Manager**.

The CCM home page opens.

2. Right-click the Server Intelligence Agent (SIA) and select **Stop**.

**Note:**

When you stop the SIA, all services managed by the SIA are stopped.

3. Right-click the SIA and select **Properties**.
4. Clear the **System Account** check box.
5. Enter the service account credentials (*DOMAINNAME\service name*) and click **OK**.
6. Restart the SIA.
7. If necessary, repeat steps 1 to 5 for each SIA running a service that must be configured.

#### 7.4.2.1.3 Preparing the application server for Windows AD authentication (Kerberos)

This section contains the tasks related to configuring Kerberos for use with these the following application servers:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.10

This section contains this information:

- The workflow specific to a particular web application server. This 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.
- Sample Krb5.ini file for Java application servers.

##### *Overview*

The specific process of configuring Kerberos for a web application server varies slightly depending the specific application server. However, the general process of configuring Kerberos involves these steps:

- Creating the Kerberos configuration file.

- Creating the JAAS login configuration file.

**Note:**

This step is not required for the SAP NetWeaver 7.10 Java application server. However you will need to add LoginModule to your SAP NetWeaver server.

- Modifying the Java Options.
- Restarting your Java application server.

*To create a Kerberos configuration file for SAP NetWeaver, Tomcat, WebLogic, SAP NetWeaver or Oracle*

Follow these steps to create the Kerberos configuration file if you're using SAP Netweaver 7.10, Tomcat 6, 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. 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:**

`DOMAIN.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. `[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`. In a multiple domain configuration, under

[libdefaults] the `default_realm` value may be any of the source domains. The best practice is to use the domain with the greatest number of users that will be authenticating with their AD accounts. If no UPN suffix is supplied at log on, it defaults to the value of `default_realm`. This value should be consistent with the **default domain** setting in the CMC.

### Related Topics

- [To modify the Java options for Kerberos on Tomcat](#)

### *To create a 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.

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.

3. Save and close the file.

### Related Topics

- [To modify the Java options for Kerberos on WebSphere](#)

### Sample multiple domain Krb5.ini file

The following is a sample file with multiple domains:

```
[domain_realm]
; trust relationship: childtest4<->sboptest3<->sboptest<->sboptest2
[libdefaults]
    default_realm = SBOPTTEST.COM
[realms]
SBOPTTEST.COM = {
    kdc = VANPGVMBOBJ01.sboptest.com
}
SBOPTTEST2.COM = {
    kdc = VANPGVMBOBJ05.sboptest2.com
}
SBOPTTEST3.COM = {
    kdc = VANPGVMBOBJ07.sboptest3.com
}
CHILDTTEST4.SBOPTTEST3.COM = {
    kdc = vanpgvmbobj08.childtest4.sboptest3.com
}
[capaths]
; for clients in sboptest3 to login sboptest2
SBOPTTEST3.COM = {
    SBOPTTEST2.COM = SBOPTTEST.COM
}
; for clients in childtest4 to login sboptest2
CHILDTTEST4.SBOPTTEST3.COM = {
    SBOPTTEST2.COM = SBOPTTEST.COM
    SBOPTTEST2.COM = SBOPTTEST3.COM
}
```

### To create a Tomcat or WebLogic 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 your java options.

2. Add the following code to your JAAS `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Save and close the file.

### To create a Oracle JAAS login configuration file

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 a WebSphere 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`
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.

### *To add a LoginModule to SAP NetWeaver*

To use Kerberos and 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 need to add a LoginModule and update some Java settings on SAP NetWeaver 7.10.

To map the `com.sun.security.auth.module.Krb5LoginModule` to the `com.businessobjects.security.jgss.initiate`, you 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 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 where you stored the file.

4. Close the Tomcat configuration file.
5. Restart Tomcat.

*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** list, and **GLOBAL** from the **Platform** list.
7. Click **System**.
8. Add the following custom parameter information:

java.security.krb5.conf	<i>&lt;path to the krb5.ini file including the file name&gt;</i>
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 the **Authentication** node and select **Create sub-node**.
14. Select **Value-Entry** from the top list.
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 need to restart your NetWeaver server.

### *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 Information platform services applications.
2. Open the script that starts the domain of WebLogic that runs your Information platform services 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.config=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 Information platform services 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 Information platform services 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.security.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 Information platform services.
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.

## 7.4.3 AD authentication single sign-on

### 7.4.3.1 Options for Windows AD authentication single sign-on

There are two supported methods for setting up single sign-on for Windows AD authentication with SAP BusinessObjects Enterprise:

- Vintela single sign on - this option can only be used with Kerberos.
- Single sign on with SiteMinder - this option can only be used with Kerberos.

### 7.4.3.2 Configuring Windows AD authentication (Kerberos) with Vintela single sign-on

The following section details the required tasks for setting up Information platform services to work with Windows AD authentication and Vintela single sign-on.

**Note:**

The prerequisite setup tasks for Windows AD authentication, together with the specific Vintela single sign-on task should be completed before configuring the Windows AD authentication options in the CMC.

### 7.4.3.3 Workflow for configuring Kerberos and single sign-on for Java BI launch pad

To set up Information platform services to work with Windows AD authentication and Vintela single sign-on you need to complete the following tasks:

1. Create and configure a service account to be used for Vintela single sign-on.
2. Setup your Information platform services deployment to run under the service account.
3. Configure the BOE general and BI launch pad-specific properties for Vintela single sign on.
4. Increase the header size limit of the Java application server.
5. Configure the Internet Browsers for Vintela single sign-on.
6. Configure constrained delegation for Vintela single sign-on (optional).

Once all these tasks have been completed you can configure the Windows AD authentication options in the CMC.

### 7.4.3.4 To set up the service account for Vintela single sign-on

You need to set up a new service account on the domain controller to successfully enable Vintela single sign-on for Windows AD authentication. This service account will be used specifically for allow users in a given Windows AD group to sign-on to BI launch pad. This task is performed on the AD domain controller machine. Steps 1-5 below are required for using Windows AD with Kerberos, while steps 6-7 are specific for setting up Vintela single sign-on.

1. Create a new service account with a password on the primary domain controller.
2. Run the kerberos keytab setup command `ktpass` to create and place a keytab file.

You will need to specify the `ktpass` parameters listed in the following table:

Parameter	Description
-out	Specifies the name of the Kerberos keytab file to generate.

Parameter	Description
-princ	Specifies principal name used for the service account. This parameter should be specified in SPN format. <b>Note:</b> The name of your service account is case-sensitive. An SPN always includes the name of the host computer on which the service instance is running. <b>Tip:</b> The SPN must be unique in the forest in which it is registered. One way to check is to use Windows support tool <code>Ldp.exe</code> to search for the SPN.
-mapuser	Specifies the name of the user account to which the -princ (above) is mapped. This is account under which the server intelligence agent runs.
-pass	Specifies the password used by the service account.
-ptype	Specifies the principal type. Should be specified as: <code>-ptype KRB5_NT_PRINCIPAL</code>
-crypto	Specifies which encryption type to use with the service account. Use the following: <code>-crypto RC4-HMAC-NT</code>

For example:

```
ktpass -out keytab_filename.keytab -princ
MYSIAMYSERVER/sbo.service.DOMAIN.COM
-mapuser sbo.serviceDOMAIN.COM -pass password
-kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

The output from the `ktpass` command should confirm the target domain controller, and that a Kerberos keytab file containing the shared secret has been created. The command also maps the principal name to the (local) service account.

- Run the `setspn -l` command to verify that the `ktpass` command was successfully executed. The display output lists all the service principal names registered to the local service account.
- Right-click the service account you created in Step 1, select **Properties > Delegation**.
- Click **Trust this user for delegation to any service (Kerberos only)**.
- Use the `setspn -a` command to add the HTTP service principal names to the service account you created in Step 1. Specify service principal names for the server, fully qualified domain server and IP address for the machine on which BI launch pad is deployed.

For example:

```
setspn -a HTTP/servername servicename
setspn -a HTTP/servernamedomain servicename
setspn -a HTTP/<ip address of server> servicename
```

Where *servername* is the name of the server on which BI launch pad is deployed and *servername domain* is the fully qualified domain name of the latter.

7. Run `setspn -l servicename` to verify that the HTTP service principal names were added to the service account.

The output for the command should include all the registered service principal names as shown in the example below:

```
Registered ServicePrincipalNames for
CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
HTTP/<ip address of server>
HTTP/servername.DOMAIN.com
HTTP/servername
servername/servicenameDOMAIN.com
```

The service account has had all the required service principal names added, and the required keytab file has been created.

For Vintela single sign-on to work, you need to setup the Information platform services servers, edit BI launch pad properties, and to copy the keytab file to the appropriate directory.

### 7.4.3.5 Preparing servers for Vintela single sign-on

Before you perform this task:

- You must ensure that the computer on which the Information platform services servers are deployed has been added to the primary domain and that all the required DNS suffixes have been appended.
  - You need the keytab file you created for Windows AD authentication with Kerberos.
1. Copy the Kerberos keytab file to a location on the computer hosting the Information platform services servers.
  2. Add the Kerberos service account to the Administrator group on the host computer.  
Format the account name as `DOMAIN_NAME\service name`.
  3. Add the Kerberos service account to the following system rights in the Local Security Policy MMC:

System right	Impact
<b>Act as part of the Operating system</b>	Allows a process to impersonate any user without the need to authenticate
<b>Log on as a Batch job</b>	Enables a user to be logged on through a batch-queue facility
<b>Log on as a service</b>	Allows a service account to register a process as a service
<b>Replace a Process Level Token</b>	Allows an account to call the CreateProcessAs-User() API, enabling one service to start another

You must run the Information platform services servers under the service account.

4. Go to **Programs > SAP BusinessObjects BI platform 4 > SAP BusinessObjects BI platform > Central Configuration Manager**.
5. In the Central Configuration Manager, right-click the Server Intelligence Agent (SIA) and select **Stop**.
6. Right-click the SIA and select **Properties**.
7. Clear the **System Account** check box.
8. Enter the Kerberos account credentials (*DOMAIN\_NAME\service name*) from step 2, and click **OK**.
9. Restart the SIA.

To complete setup of Vintela single sign-on:

- Prepare the web application server and BI launch pad properties for Vintela single sign-on.
- Configure the Windows AD security plugin to enable Windows AD authentication and Vintela single sign-on.

### 7.4.3.6 To enable Vintela single sign-on for BI launch pad and OpenDocument

This procedure can be used for both the BI launch pad and OpenDocument web applications. In addition to specifying Vintela single sign-on settings for the Windows AD security plugin, Vintela settings must be specified for the BOE.war properties.

1. Access the custom folder for the BOE web application on the machine hosting the web application server.

If you are using the Tomcat web application server provided with the Information platform services installation, you can directly access the following folder:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
```

**Tip:**

If you are using a web application server that does not enable direct access to the deployed web applications, you can use the following folder in your product installation to modify the BOE web application.

```
<INSTALLDIR>\Information platform services XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

You will have to later redeploy the modified BOE web application.

2. Create a new file.

**Note:**

Use Notepad or any other text-editing utility.

3. Enter the following:

```
sso.enabled=true  
siteminder.enabled=false  
vintela.enabled=true  
idm.realm=[YOUR_REALM]  
idm.princ=[YOUR_PRINCIPAL]  
idm.allowUnsecured=true
```

```
idm.allowNTLM=false
idm.logger.name=simple
idm.logger.props=error-log.properties
```

**Note:**

The `idm.realm` and `idm.princ` parameters require valid values. The `idm.realm` should be the same value you set when you configured the `default_realm` in your `krb5.ini` file. The value must be in upper case. The `idm.princ` parameter is the SPN used to for the service account created for Vintela single sign-on.

4. If you have chosen to use a keytab file, add the `keytab` parameter and specify the path to the file as shown in the example below:

```
idm.keytab=C:/WIN/filename.keytab
```

Skip the following step if you do not want to use constrained delegation for Windows AD authentication and Vintela single sign-on.

5. To use constrained delegation add:

```
idm.allowS4U=true
```

6. Close the file and save it with a `global.properties` name:

**Note:**

Make sure the file name is not saved under any extensions such as `.txt`.

7. Create another file in the same directory. Save the file as `OpenDocument.properties` or `BI launchpad.properties` depending on your requirements.
8. Enter the following statement:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

For example:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

9. Save and close the file.
10. Restart your web application server.

The new properties will take effect only after the BOE web application is redeployed on the machine running the web application server. Use `WDeploy` to redeploy BOE on the web application server. For more information on using `WDeploy` to undeploy web applications, see the *Information Platform Services Web Application Deployment Guide*.

**Note:**

If your deployment is using a firewall, remember to open all the required ports otherwise the web applications will not be able to connect to the Information platform services servers.

**Related Topics**

- [Preparing the application server for Windows AD authentication \(Kerberos\)](#)
- [Sample multiple domain Krb5.ini file](#)

### 7.4.3.7 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 Information platform services on Windows, and you did not modify the default installation location, replace `<TomcatINSTALLDIR>` with `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\`
- 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.

### 7.4.3.8 Configuring Internet browsers

To support Kerberos single sign-on, you must configure Information platform services clients. This involves configuring the Internet Explorer (IE) browser on the client machines.

#### 7.4.3.8.1 To configure Internet Explorer on the client machines

You need to configure the Internet Explorer browser on a Information platform services client machine to support end-to-end single sign-on. This implementation includes the following tasks:

- Configuring client machines for integrated Windows authentication
- Adding the URL for BI launch pad to the list of 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 the URL for BI launch pad 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 URL for BI launch pad, and click **Add**.
  - 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.

#### 7.4.3.8.2 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 BI launch pad. For example if your BI launch pad URL is `http://machine.domain.com:8080/BOE/BI`, then you will need to enter `http://machine.domain.com`.

**Note:**

To add more than one URL, separate them with a comma. For example: `http://machine.domain.com,machine2.domain.com`.

- e. Click **OK**.

**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 BI launch pad. For example if your BI launch pad URL is `http://machine.domain.com:8080/BOE/BI`, then you will need to enter `http://machine.domain.com`.

**Note:**

To add more than one URL, separate them with a comma. For example: `http://machine.domain.com,machine2.domain.com`.

- e. Click **OK**.

3. Close and reopen the Firefox browser window for these changes to take effect.
4. Repeat all of these steps on each Information platform services client machine.

### 7.4.3.9 To configure constrained delegation for Vintela single sign-on

Constrained delegation is optional for AD authentication and Vintela single sign-on. It is required for deployment scenarios that involve single sign-on to the system database.

1. On the AD domain controller machine, open the Active Directory "Users and Computers" snap-in.
2. Right-click the service account you created for Vintela single sign-on, and click **Properties > Delegation**.
3. Select **Trust this user for delegation to the specified services only**.
4. Select **Use Kerberos only**.
5. Click **Add > Users or Computers**.
6. Type the service account name (used for Vintela single sign-on) and click **OK**.  
A list of services is displayed.
7. Select the following services and then click **OK**.
  - The HTTP service
  - The service used to run the Service Intelligence Agent (SIA) on the machine hosting SAP BusinessObjects Enterprise.

The services are added to the list of services that can be delegated for the (Vintela single sign-on) account.

You need to modify the web application properties to account for this modification. Open the BOE global.properties file on your web application server. Add the following and then restart the web application server.

```
idm.allowS4U=true
```

### 7.4.3.10 Using Windows AD with SiteMinder

This section explains how to use AD and SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the AD security plug-in to create single sign-on to Information platform services. You can use SiteMinder with Kerberos.

Ensure your SiteMinder identity management resources are installed and configured before configuring Windows AD authentication to work with SiteMinder. For more information about SiteMinder and how to install it, refer to your SiteMinder documentation.

There are two tasks you must complete to enable AD single sign-on with SiteMinder:

- Configure the AD plug-in for single sign-on with SiteMinder
- Configure SiteMinder properties for the BOE web application

**Note:**

Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done regardless of which supported version of SiteMinder you are using. For more information about SiteMinder configuration, refer to your SiteMinder documentation.

#### 7.4.3.10.1 To modify the BOE properties file for Windows AD authentication with SiteMinder

In addition to specifying SiteMinder settings for the Windows AD security plugin, SiteMinder settings must be specified for the BOE.war properties.

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

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Create a new file.

**Note:**

Use Notepad or another text-editing utility.

3. Enter the following statement:

```
sso.enabled=true  
siteminder.authentication=secWinAD  
siteminder.enabled=true
```

4. Save the file with the name `global.properties`, and close the file.

**Note:**

Make sure the file name is not saved with an extension, such as `.txt`.

5. Create another file in the same directory.
6. Enter the following statement:

```
authentication.default=secWinAD  
cms.default=[CMS name]:[CMS port number]
```

For example:

```
authentication.default=LDAP  
cms.default=mycms:6400
```

7. Save the file with the name `BIlaunchpad.properties`, and close the file.

The new properties will take effect only after `BOE.war` is redeployed on the computer running the web application server. Use `WDeploy` to redeploy the WAR file on the web application server. For more information on using `WDeploy` to undeploy web applications, see the *Information Platform Services Web Application Deployment Guide*.

#### 7.4.3.10.2 To disable SiteMinder

If you want to prevent SiteMinder from being configured, or to disable it after it has been configured in the CMC, modify the web configuration file for BI launch pad.

##### *To disable SiteMinder for Java clients*

In addition to disabling SiteMinder settings for the Windows AD security plugin, SiteMinder settings must be disabled for the `BOE.war` file on your web application server.

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

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Open the `global.properties` file.
3. Change `siteminder.enabled` to `false`

```
siteminder.enabled=false
```

4. Save your changes and close the file.

The change takes effect only after `BOE.war` is redeployed on the machine running the web application server. Use `WDeploy` to redeploy the WAR file on the web application server. For more information on using `WDeploy` to undeploy web applications, see the *Information platform services Web Application Deployment Guide*.

## 7.4.4 Mapping AD groups and configuring AD authentication

### 7.4.4.1 To map AD users and groups and configure the Windows AD security plugin

To configure Windows AD authentication to work with a specific authentication type, first complete all required preparatory tasks. For information, see “Related Topics” below.

Regardless of which protocol is used, you must complete the following steps to allow AD users to authenticate. Follow steps 1 to 8 below to import AD groups to Information platform services.

1. In the "Authentication" management area of the CMC, double-click **Windows AD**.
2. Click the **Enable Windows Active Directory (AD)** check box.
3. Under "AD Configuration Summary", click the link beside **AD Administration Name**.

**Note:**

Before the Windows AD plugin 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.

4. Enter the name and password of an enabled domain user account, using one of the following formats:
  - NT name: `DomainName\UserName`
  - UPN: `user@DNS_domain_name`

Information platform services uses this account to query information from AD. It does not modify, add, or delete content from AD; it only reads information.

**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.

5. Enter information in the **Default AD Domain** box.

You can map groups from the default domain, 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 logging on to Information platform services via AD authentication.

6. Under "Mapped AD Member Groups", enter the AD domain\group in the **Add AD Group (Domain\Group)** box, 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:**

To map a local group, use only the NT name format (`\\ServerName\GroupName`). AD does not support local users; local users who belong to a mapped local group are not mapped to Information platform services. Therefore, they are not able to access the system.

7. Click **Add**.

The group is added to the list.

**Note:**

To import AD group accounts without configuring AD authentication options or AD group updates, skip steps 8 to 18.

8. If you selected **Use Kerberos authentication**:

- a. To configure single sign-on to a database, select **Cache security context**.
- b. In the **Service principal name** box, enter the SPN mapped to the service account.

**Note:**

To configure Information platform services for Kerberos and AD authentication using Kerberos, you must have a service account. You can either create a domain account or use an existing domain account. The service account will be used to run the Information platform services servers. To enable AD authentication with Vintela single sign-on, you must provide an SPN that is configured for this purpose.

**Tip:**

When manually logging on to BI launch pad, users from other domains must append the domain name (in uppercase letters) after the user name—for example, user@CHILD.PARENTDOMAIN.COM.

9. To configure single sign-on, select **Enable Single Sign On for selected authentication mode**.

To enable single sign-on, you must also configure the BOE web application general properties and BI launch pad properties.

10. Under "Synchronization of Credentials", select an option and update the AD user's data source credentials at logon time.

This synchronizes the data source with the user's current logon credentials

11. To configure SiteMinder as the single sign-on option for AD authentication using Kerberos, under "SiteMinder Options":

**Note:**

You can configure either Vintela or SiteMinder as the single sign-on option. Clear all entries in the **Service principal name** box (step 9b) if you want to configure SiteMinder options.

a. Click **Disabled**.

The "Windows AD SiteMinder configuration" page appears. If you have not configured the Windows AD plug-in, when asked if you want to continue, click **OK**.

b. Click **Use SiteMinder Single Sign On**.

c. In the **Policy Server Host** box, type the name of each policy server, and click **Add**.

d. For each **Policy Server Host**, specify the **Accounting**, **Authentication**, and **Authorization** port numbers.

e. Enter the name of the **Agent Name** and the **Shared Secret**, and enter the **Shared Secret** again.

**Note:**

Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done, regardless of which supported version of SiteMinder you are using. For information about SiteMinder and how to install it, see the SiteMinder documentation.

f. Click **Update** to save your information and return to the main AD authentication page.

12. Under "AD Alias Options", specify how to add new aliases to and update aliases in Information platform services:
  - a. Under "New Alias Options", specify how to map new aliases to Enterprise accounts:
    - **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 to create a new account for each user.
  - b. Under "Alias Update Options", specify how to manage alias updates for Enterprise accounts:
    - **Create new aliases when the Alias Update occurs**

Use this option to automatically create a new alias for every AD user mapped to Information platform services. New AD accounts are added for users without Information platform services 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 Information platform services. Information platform services 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 Information platform services.
  - c. If your Information platform services license is based on users roles, under "New User Options", specify how new users are created:
    - **BI Viewer User**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.
    - **BI Analyst User**

New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all applications workflows that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.
  - d. If your Information platform services license is not based on users roles, under "New User Options", specify how new users are created:
    - **New users are created as named users**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

- **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 Information platform services 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 Information platform services, a 100-user concurrent license could support 250, 500, or 700 users.

**13.** To configure how to schedule AD alias updates:

- a. Click **Schedule**.
- b. In the "Schedule" dialog box, select a recurrence in the **Run object** list.
- c. Set schedule options and parameters as needed.
- d. Click **Schedule**.

When the alias update occurs, the group information is also updated.

**14.** Under "Attribute Binding Options", specify the attribute binding priority for the AD plugin:

- a. Click the **Import Full Name, Email Address and other attributes** box.  
The full names and descriptions used in the AD accounts are imported and stored with the user objects in Information platform services.
- b. Specify an option for **Set priority of AD attribute binding relative to other attributes binding**.  
When this option is set to **1**, AD attributes take priority in scenarios where AD and other plugins (LDAP and SAP) are enabled. When it is set to **3**, attributes from other enabled plugins take priority.

**15.** Under "AD Group Options", configure AD group updates:

- a. Click **Schedule**.  
The "Schedule" dialog box appears.
- b. Select a recurrence in the **Run object** list.
- c. Set the remaining schedule options and parameters as needed.
- d. Click **Schedule**.

The system schedules and runs the update according to the schedule information you specified. You can view the next scheduled update for AD group accounts under "AD Group Options".

**16.** Under "On-Demand AD Update", select one of the following options:

- **Update AD Group now**

Select this option if you want to update the AD groups. The updates start after you click **Update**.

**Note:**

This option affects any scheduled AD group updates. The next scheduled AD group update is listed under "AD Group Options".

- **Update AD Groups and Aliases now**

Select this option if you want to update the AD group and user aliases. The updates start after you click **Update**.

**Note:**

This option affects any scheduled AD group updates. The next scheduled updates are listed under "AD Group Options" and "AD Alias Options".

- **Do not update AD Groups and Aliases now**

Select this option if you do not want to update AD groups and user aliases. If you click **Update**, neither the group nor the user aliases will be updated.

**Note:**

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

17. Click **Update**, and click **OK**.

**Related Topics**

- [Single sign-on with Windows AD](#)
- [Using Windows AD with SiteMinder](#)
- [Using Kerberos authentication for Windows AD](#)

## 7.4.5 Troubleshooting Windows AD authentication

### 7.4.5.1 Troubleshooting your Kerberos configuration

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Java SDK Kerberos configuration

#### 7.4.5.1.1 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\\.businessobjects\jce_verbose.log
```

#### 7.4.5.1.2 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>\SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

For example:

```
C:\Program Files\SAP BusinessObjects\SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

The domain and service principal name are case-sensitive. If the problem persists, confirm that the domain and service principal name exactly match the domain and service principal name the Active Directory.

#### 7.4.5.1.3 Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to Information platform services. Despite this fact, they are unable to successfully log onto the CMC or BI launch pad with Windows AD authentication and Kerberos in the following format: DOMAIN\ABC123

This problem can happen when the user is set up in Active Directory with a UPN and SAM name that are not exactly the same. The following examples may cause a problem:

- The UPN is abc123@company.com but the SAM name is DOMAIN\ABC123.
- The UPN is jsmith@company but the SAM name is DOMAIN\johnsmith.

There are two ways to address this problem:

- Have users log in using the UPN name rather than the SAM name.
- Ensure the SAM account name and the UPN name are the same.

#### 7.4.5.1.4 Pre-authentication error

A user who has previously been able to log on, can no longer log on successfully. The user will receive this error: Account Information Not Recognized. The Tomcat error logs reveal the following error: "Pre-authentication information was invalid (24)"

This can occur because the Kerberos user database didn't get a change made to UPN in AD. This may mean that the Kerberos user database and the AD information are out of sync.

To resolve this problem, reset the user's password in AD. This will ensure the changes are propagated correctly.

#### **Note:**

This problem is not an issue with J2SE 5.0.

## 7.5 SAP authentication

### 7.5.1 Configuring SAP authentication

This section explains how to configure Information platform services authentication for your SAP environment.

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

#### Accessing the SAP authentication application

You must provide Information platform services with information about your SAP system. Information platform services installs a web application to assist you. This web application is accessible through the main Information platform services administration tool, the Central Management Console (CMC). To access it from the home page of the CMC, click **Authentication**.

#### Authenticating SAP users

Security plug-ins expand and customize the ways in which Information platform services authenticates users. The SAP Authentication feature includes an SAP security plug-in (`secSAPR3.dll`) for the Central Management Server (CMS) component of Information platform services. This SAP security plug-in offers several key benefits:

- It acts as an authentication provider that verifies user credentials against your SAP system on behalf of the CMS. When users log on to Information platform services directly, they can choose SAP Authentication and provide their usual SAP user name and password. Information platform services can also validate Enterprise Portal logon tickets against SAP systems.
- It facilitates account creation by allowing you to map roles from SAP to Information platform services user groups, and it facilitates account management by allowing you to assign rights to users and groups in a consistent manner within Information platform services.
- It dynamically maintains SAP role listings. So, once you map an SAP role to Information platform services, all users who belong to that role can log on to Information platform services. When you make subsequent changes to the SAP role membership, you need not update or refresh the listing in Information platform services.
- The SAP Authentication component includes a web application for configuring the plug-in. You can access this application in the "Authentication" area of the Central Management Console (CMC).

## 7.5.2 Creating a user account for Information platform services

The Information platform services system requires an SAP user account that is authorized to access SAP role membership lists and authenticate SAP. You will need the account credentials to connect Information platform services to your SAP system. For general instruction on creating SAP user accounts and assigning authorizations through roles, see your SAP BW documentation.

Use transaction `SU01` to create a new SAP user account named `CRYSTAL`. Use transaction `PFCG` to create a new role named `CRYSTAL_ENTITLEMENT`. (These names are recommended but not required.) Change the new role's authorization data by setting these values for the following authorization objects:

Authorization object	Field	Value
Authorization for file access (S_DATASET)	Activity (ACTVT)	Read, Write (33, 34)
	Physical file name (FILENAME)	* (denotes All)
	ABAP program name (PROGRAM)	*
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)

Authorization object	Field	Value
User Master Maintenance: User Groups (S_USER_GRP)	Activity (ACTVT)	Create or Generate, and Display (03)
	User group in user master maintenance (CLASS)	* <b>Note:</b> For greater security, you may prefer to explicitly list the user groups whose members require access to Information platform services.

Finally, add the `CRYSTAL` user to the `CRYSTAL_ENTITLEMENT` role.

**Tip:**

If your system policies require users to change their passwords when they first log on to the system, log on now with the `CRYSTAL` user account and reset its password.

## 7.5.3 Connecting to SAP entitlement systems

Before you can import roles or publish BW content to Information platform services, you must provide information about the SAP entitlement systems to which you want to integrate. Information platform services uses this information to connect to the target SAP system when it determines role memberships and authenticates SAP users.

### 7.5.3.1 To add an SAP entitlement system

1. Go to the "Authentication" management area of the CMC.
2. Double-click the **SAP** link.

The entitlement systems settings appear.

**Tip:**

If an entitlement system is already displayed in the **Logical system name** list, click **New**.

3. In the **System** field, type the three-character System ID (SID) of your SAP system.

4. In the **Client** field, type the client number that Information platform services must use when it logs on to your SAP system.

Information platform services combines your System and Client information, and adds an entry to the **Logical system name** list.

5. Ensure the **Disabled** check box is clear.

**Note:**

Use the **Disabled** check box to indicate to Information platform services that a particular SAP system is temporarily unavailable.

6. Complete the **Message Server** and **Logon Group** fields as appropriate, if you have set up load balancing such that Information platform services must log on through a message server .

**Note:**

You must make the appropriate entries in the `Services` file on your Information platform services machine to enable load balancing - especially if your deployment not on a single machine. Specifically you should account for the machines hosting the CMS, the Web application server, as well as all machines managing your authentication accounts and settings.

7. If you have not set up load balancing (or if you prefer to have Information platform services log on directly to the SAP system), complete the **Application Server** and **System Number** fields as appropriate.
8. In the **User name**, **Password**, and **Language** fields, type the user name, password, and language code for the SAP account that you want Information platform services to use when it logs on to SAP.

**Note:**

These credentials must correspond to the user account that you created for Information platform services.

9. Click **Update**.

If you add multiple entitlement systems, click the **Options** tab to specify the system that Information platform services uses as the default (that is, the system that is contacted to authenticate users who attempt to log on with SAP credentials but without specifying a particular SAP system).

**Related Topics**

- [To create a user account](#)

### 7.5.3.2 To verify if your entitlement system was added correctly

1. Click the **Role Import** tab.
2. Select the name of the entitlement system from the **Logical system name** list.

If the entitlement system was added correctly, the **Available roles** list will contain a list of roles that you can choose to import.

**Tip:**

If no roles are visible in the **Logical system name** list, look for error messages on the page. These may give you the information you need to correct the problem.

### 7.5.3.3 To temporarily disable a connection to an SAP entitlement system

In the CMC, you can temporarily disable a connection between Information platform services and an SAP entitlement system. This may be useful to maintain the responsiveness of Information platform services in cases such as the scheduled down time of an SAP entitlement system.

1. In the CMC, go to the **Authorization** management area.
2. Double-click the **SAP** link.
3. In the **Logical system name** list, select the system you want to disable.
4. Select the **Disabled** check box.
5. Click **Update**.

## 7.5.4 Setting SAP Authentication options

SAP Authentication includes a number of options that you can specify when integrating Information platform services with your SAP system. The options include:

- Enabling or disabling SAP authentication
- Specifying connection settings
- Linking imported users to Information platform services license models.
- Configuring single sign-on to the SAP system

### 7.5.4.1 To set SAP Authentication options

1. Go to the "Authentication" management area of the CMC.
2. Double-click the **SAP** link, and click the **Options** tab.
3. Review and modify settings as required.

Setting	Description
<b>Enable SAP Authentication</b>	Clear this check box if you want to disable SAP Authentication. To disable SAP Authentication for a specific SAP system, select the system's <b>Disabled</b> check box on the <b>Entitlement Systems</b> tab.)
<b>Content folder root</b>	Specify where you want Information platform services to begin replicating the BW folder structure in the CMC and BI launch pad. The default is <code>/SAP/2.0</code> but you can change it to a different folder. To change this value, you must change it in the CMC and in Content Administration Workbench.
<b>Default system</b>	<p>Select the SAP entitlement system that Information platform services uses as the default (that is, the system that is contacted to authenticate users who attempt to log on with SAP credentials but without specifying a particular SAP system).</p> <p><b>Note:</b> If you designate a default system, users from that system do not have to enter their System ID and client when they connect from client tools like Live Office or Universe Designer using SAP authentication. For example, if SYS~100 is set as the default system, SYS~100/user1 would be able to log on as user1 when SAP authentication is chosen.</p>
<b>Max. number of failed attempts to access entitlement system</b>	<p>Type the number of times that Information platform services should re-attempt contacting an SAP system to fulfill authentication requests. Setting the value to <code>-1</code> allows Information platform services to attempt to contact the entitlement system an unlimited number of times. Setting the value to <code>0</code> limits Information platform services to making one attempt to contact the entitlement system.</p> <p><b>Note:</b> Use this setting together with <b>Keep entitlement system disabled [seconds]</b> to configure how Information platform services handles SAP entitlement systems that are temporarily unavailable. Information platform services uses these settings to determine when to stop communicating with an SAP system that is unavailable, and when it should resume communication with that system.</p>

Setting	Description
<b>Keep entitlement system disabled [seconds]</b>	Type the number of seconds that Information platform services should wait before resuming attempts to authenticate users against the SAP system. For example, if you type 3 for <b>Max failed entitlement system accesses</b> , Information platform services allows a maximum of 3 failed attempts to authenticate users against any particular SAP system; the fourth failed attempt results in Information platform services ceasing its attempts to authenticate users against that system for the amount of time specified.
<b>Max. concurrent connections per system</b>	Specify how many connections you want to keep open to your SAP system at the same time. For example, if you type 2 in this field, Information platform services keeps two separate connections open to SAP.
<b>Number of uses per connection</b>	Specify how many operations you want to allow to the SAP system per connection. For example, if you specified 2 for <b>Max concurrent connections per system</b> and 3 for <b>Number of uses per connection</b> , once there have been three logons on one connection, Information platform services closes that connection and restart it.
<b>BI Viewer and BI Analyst</b>	<p>Specify whether new user accounts are configured under either the BI Viewer or BI Analyst user roles. The BI Viewer role is typically assigned to users who are content consumers. This role has restricted access to application workflows as stipulated in the Information platform services license agreement. The BI Analyst role is for users who create and modify content for Information platform services applications. This role does not have restricted access to application workflows.</p> <p><b>Note:</b> The option you select here does not change the number or type of user licenses that you have installed in Information platform services. You must have the appropriate licenses available on your system.</p>

Setting	Description
<b>Concurrent users and Named Users</b>	<p>Specify whether new user accounts are configured to use concurrent user licenses or named user licenses. Concurrent licenses specify the number of people who can connect to Information platform services at the same time. This type of licensing is very flexible because a small number of concurrent licenses can support a large user base. For example, depending on how often and how long users access Information platform services, a 100 user concurrent license could support 250, 500, or 700 users. 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.</p> <p><b>Note:</b> The option you select here does not change the number or type of user licenses that you have installed in Information platform services. You must have the appropriate licenses available on your system.</p>
<b>Import Full Name, Email Address and other attributes</b>	<p>Select this option if you want to specify a priority level for the SAP authentication plugin. The full names and descriptions used in the SAP accounts are imported and stored with the user objects in Information platform services.</p>
<b>Set priority of SAP attribute binding relative to other attributes binding</b>	<p>Specifies a priority for binding SAP user attributes (full name and email address). If the option is set to 1, SAP attributes take priority in scenarios where SAP and other plugins (Windows AD and LDAP) are enabled. If the option is set to 3, attributes from other enabled plugins take priority.</p>

Use the following options to configure the SAP single sign-on service:

Option	Description
<b>System ID</b>	The system identifier provided by Information platform services to the SAP system when performing the SAP single sign-on service.
<b>Browse</b>	Use this button to upload the key store file generated to enable the SAP single sign-on. You can also manually enter the full path to the file in the field provided.
<b>Key Store Password</b>	Provide the password required to access the key store file.
<b>Private Key Password</b>	Provide the password required to access the certificate corresponding to the key store file. The certificate is stored on the SAP system.
<b>Private Key Alias</b>	Provide the alias required to access the key store file.

4. Click **Update**.

#### Related Topics

- [Role-based licensing](#)
- [Configuring SAP authentication](#)

### 7.5.4.2 To change the Content folder root

1. Go to the "Authentication" management area of the CMC.
2. Double-click the **SAP** link.
3. Click **Options** and type the name of the folder in **Content folder root** field.  
The folder name that you type here is the folder that you want Information platform services to begin replicating the BW folder structure from.
4. Click **Update**.
5. In the BW Content Administration Workbench, expand **Enterprise system**.
6. Expand **Available systems** and double-click the system that your Information platform services is connecting to.
7. Click the **Layout** tab and in the **Content base folder**, type the folder that you want to use as the root SAP folder in Information platform services (for example, `/SAP/2.0/`).

## 7.5.5 Importing SAP roles

By importing SAP roles into Information platform services, you allow role members to log on to Information platform services with their usual SAP credentials. In addition, single sign-on is enabled so that SAP users are logged on to Information platform services automatically when they access reports from within the SAP GUI or an SAP Enterprise Portal.

### Note:

There are often many requirements for enabling SSO. Some of these might include using a driver and application that are SSO-capable, and ensuring your server and web server are in the same domain.

For each role that you import, Information platform services generates a group. Each group is named with the following convention: *SystemID~ClientNumber@NameOfRole*. You can view the new groups in the "Users and Groups" management area of the CMC. You can also use these groups to define object security within Information platform services.

Consider three main categories of users when configuring Information platform services for publishing, and when importing roles to Information platform services:

- Information platform services administrators

Enterprise administrators configure the Information platform services system for publishing content from SAP. They import the appropriate roles, create necessary folders, and assign rights to those roles and folders in Information platform services.

- Content publishers

Content publishers are those users who have rights to publish content into roles. The purpose of this category of user is to separate regular role members from those users with rights to publish reports.

- Role members

Role members are users who belong to "content bearing" roles. That is, these users belong to roles to which reports are published. They have **View**, **View on Demand**, and **Schedule** rights for any reports published to the roles they are members of. However, regular role members cannot publish new content, nor can they publish updated versions of content.

You must import all content publishing and all content bearing roles to Information platform services prior to publishing for the first time.

### Note:

It is strongly recommended that you keep the activities of roles distinct. For example, while it is possible to publish from an administrator role, it is better practice to publish only from content publisher roles. Additionally, the function of content publishing roles is only to define which users can publish content. Thus, content publishing roles should not contain any content; content publishers should publish to content bearing roles that are accessible to regular role members.

**Related Topics**

- [How rights work in Information platform services](#)
- [Managing security settings for objects in the CMC](#)

**7.5.5.1 To import SAP roles**

1. Go to the "Authentication" management area of the CMC.
2. Double-click the **SAP** link.
3. On the **Options** tab, select **BI Viewer**, **BI Analyst**, **Concurrent users**, or **Named users** depending on your license agreement.  
Note that the option you select here does not change the number or type of user licenses that you have installed in Information platform services. You must have the appropriate licenses available on your system.
4. Click **Update**.
5. On the **Role Import** tab, select the appropriate entitlement system in the **Logical system name** list.
6. In the "Available roles" area, select the role(s) that you want to import and click **Add**.
7. Click **Update**.

**7.5.5.2 To verify that roles and users were imported correctly**

Before starting this task, you must know the user name and password of an SAP user who belongs to a role you mapped to Information platform services.

1. For Java BI launch pad, go to `http://WebServer:PortNumber/BOE/BI`.  
Replace *webserver* with the name of the web server and *portnumber* with the port number that is set up for Information platform services. You may need to ask your administrator for the name of the web server, the port number, or the URL to enter.
2. In the **Authentication Type** list, select **SAP**.  
By default, the **Authentication Type** list is hidden in BI launch pad. The administrator must enable it in the `BIlaunchpad.properties` file and then restart the app server.
3. Enter the SAP system and the system client that you want to log on to.
4. Enter the user name and the password of a mapped user.
5. Click **Log On**.  
You are logged on to BI launch pad as the selected user.

### 7.5.5.3 Updating SAP roles and users

After enabling SAP authentication, it is necessary to schedule and run regular updates on mapped roles that have been imported into Information platform services. This will ensure that your SAP role information is accurately reflected in Information platform services.

There are two options for running and scheduling updates for SAP roles:

- **Update roles only:** using this option will only update the links between the currently mapped roles that have been imported in Information platform services. It is recommended that you use this option if you expect to run frequent updates, and you have concerns over system resource usage. No new user accounts will be created if you only update SAP roles.
- **Update roles and aliases:** this option not only updates links between roles but will also create new user accounts in Information platform services for user aliases added to roles in the SAP system.

**Note:**

If you have not specified to automatically create user aliases for updates when you enabled SAP authentication, no accounts will be created for new aliases.

#### 7.5.5.3.1 To schedule updates for SAP roles

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

1. Click the **User Update** tab.
2. Click **Schedule** under either "Update Roles Only" or "Update Roles and Aliases".

**Tip:**

To immediately run an update, click **Update Now**.

**Tip:**

Select **Update Roles Only** if you want frequent updates or have concerns about system resources. It takes the system longer to update both roles and aliases.

The "Recurrence" dialog box appears.

3. Select an option in the **Run Object** list, and enter scheduling information.

You can choose the following recurrence patterns:

Recurrence pattern	Description
<b>Hourly</b>	The update will be run every hour. You specify at what time it will start, as well as a start and end date.
<b>Daily</b>	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.

Recurrence pattern	Description
<b>Weekly</b>	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 a start and end date.
<b>Monthly</b>	The update will be run every month or every several months. You can specify what time it will run, as well as a start and end date.
<b>Nth Day of Month</b>	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.
<b>1st Monday of Month</b>	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
<b>Last Day of Month</b>	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
<b>X Day of Nth Week of the Month</b>	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
<b>Calendar</b>	The update will be run on the dates specified in a calendar that has previously been created.

#### 4. Click **Schedule**.

The date of the next scheduled role update appears on the **User Update** tab.

**Note:**

To cancel the next scheduled update, click **Cancel Scheduled Updates** in the "Update Roles Only" area or the "Update Roles and Aliases" area.

## 7.5.6 Setting up single sign-on to the SAP system

To enable single sign-on to the SAP system, you need to create a keystore file and a corresponding certificate. Use the keytool command line program to generate the file and the certificate. By default the keytool program is installed in the sdk/bin directory for each platform.

The certificate needs to be added to your SAP ABAP BW system, and Information platform services using the CMC.

**Note:**

The SAP authentication plugin must be configured before you can set up single sign-on to the SAP database.

### 7.5.6.1 To generate the keystore file

The PKCS12Tool program is used to generate keystore files and certificates that are required for setting up single sign-on to the SAP database. The following table lists the default locations for the PKCS12Tool.jar for each supported platform:

Platform	Default location
Windows	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib
Unix	sap_bobj/enterprise_xi40/java/lib

1. Launch a command prompt and navigate to the directory where the PKCS12Tool program is located
2. To generate the keystore file with default settings run the following command:

```
java -jar PKCS12Tool.jar
```

The files cert.der and keystore.p12 are generated in the same directory. The files contain the following default values:

Parameter	Default
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

**Tip:**

To override the default values, run the tool together with the -? parameter. The following message is displayed:

```
Usage: PKCS12Tool <options>
  -keystore <filename(keystore.p12)>
  -alias <key entry alias(myalias)>
  -storepass <keystore password(123456)>
  -dname <certificate subject DN(CN=CA)>
  -validity <number of days(365)>
  -cert <filename(cert.der)>
  (No certificate is generated when importing a keystore)
  -disablefips
  -importkeystore <filename>
```

You can use the parameters to override the default values.

### 7.5.6.2 To export the public key certificate

You need to create and export a certificate for the keystore file.

1. Launch a command prompt and navigate to the directory where the keytool program is located
2. To export a key certificate for the keystore file use the following command:

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>  
-alias <alias>
```

Replace <keystore> with the name of the keystore file.
Replace <filename> with the name of the certificate.
Replace <alias> with the alias used to create the keystore file.

3. When prompted, enter the password you provided for the keystore file.

You now have a keystore file and a certificate in the directory where the keytool program is located.

### 7.5.6.3 Importing the certificate file into the target ABAP SAP system

You need a key store file and an associated certificate for your Information platform services deployment to perform the following task.

**Note:**

This action can only be performed on an ABAP SAP system.

1. Connect to your SAP ABAP BW system using the SAP GUI.

**Note:**

You should connect as a user with administrative privileges.

2. Execute STRUSTSSO2 in the SAP GUI.

The system is prepared for importing the certificate file.

3. Go to the **Certificate** tab.

4. Ensure the **Use Binary option** box is selected.

5. Click the file path button to point to the location where the certificate file is located.

6. Click the green check mark.

The certificate file is uploaded.

7. Click **Add to Certificate List**.

The certificate is displayed in the Certificate List.

8. Click **Add to ACL** and then specify a SystemID and Client.  
The system ID must be the same used to identify the Information platform services system to SAP BW.  
The certificate is added to the Access Control List (ACL). The client should be specified as "000".
9. Save your setting and exit.  
The changes are saved in the SAP system.

### 7.5.6.4 To set up single sign-on to the SAP database in the CMC

To perform the following procedure you need to access the SAP security plugin using an administrator account.

1. Go to the "Authentication" management area of the CMC.
2. Double-click the **SAP** link and then click the **Options** tab.  
If no certificate has been imported the following message should be displayed in the "SAP SSO Service" section:  
`No key store file has been uploaded`
3. Specify System ID for your Information platform services system in the field provided.  
This should be identical to the value used when importing the certificate in the target SAP ABAP system.
4. Click the **Browse** button to point to the key store file.
5. Provide the following required details:

Field	Required information
"Key Store Password"	Provide the password required to access the key store file. This password was specified when creating the key store file.
"Private Key Password"	Provide the password required to access the certificate corresponding to the key store file. This password was specified when creating the certificate for the key store file.
"Private Key Alias"	Provide the alias required to access the key store file. This alias was specified when creating the key store file.

6. Click **Update** to submit your settings.  
Once the settings are submitted successfully, the following message is displayed under the SystemID field:  
`Key store file have been uploaded`

### 7.5.6.5 To add Security Token Service to the Adaptive Processing Server

In a clustered environment, the Security Token Services added separately to each Adaptive Processing Server.

1. In the "Servers" management area of the CMC, double-click **Core Services**.  
A list of servers appears under "Core Services".
2. Right-click the Adaptive Processing Server and click **Stop Server**.  
Do not proceed until the server state is marked as "Stopped".
3. Right-click the Adaptive Processing Server and click **Select Services**.  
The "Select Services" dialog box appears.
4. Using the **add** button, move **Security Token Service** from the **Available services** list on the left to the **Services** list on the right.
5. Click **OK**.
6. Restart the Adaptive Processing Server.

## 7.6 PeopleSoft authentication

### 7.6.1 Overview

To use your PeopleSoft Enterprise data with Information platform services , you must provide the program with information about your deployment. This information allows Information platform services to authenticate users so that they can use their PeopleSoft credentials to log on to the program.

### 7.6.2 Enabling PeopleSoft Enterprise authentication

To allow PeopleSoft Enterprise information to be used by Information platform services, Information platform services needs information on how to authenticate into your PeopleSoft Enterprise system.

### 7.6.2.1 To enable PeopleSoft Enterprise authentication in Information platform services

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click **Authentication**.
3. Double-click **PeopleSoft Enterprise**.  
The "PeopleSoft Enterprise" page appears. It has four tabs: **Options**, **Domains**, **Roles**, and **User Update**.
4. On the **Options** tab, select the **Enable PeopleSoft Enterprise Authentication** check box.
5. Make appropriate changes under **New Alias**, **Update Options**, and **New User Options** according to your Information platform services deployment. Click **Update** to save your changes before proceeding to the **Systems** tab.
6. Click the **Servers** tab.
7. In the "PeopleSoft Enterprise System User" area, type a database User name and Password for Information platform services to use to log on to your PeopleSoft Enterprise database.
8. In the "PeopleSoft Enterprise Domain" area, enter the Domain name and QAS address used to connect to your PeopleSoft Enterprise environment, and click **Add**.

**Note:**

If you have multiple PeopleSoft domains, repeat this step for any additional domains you want to have access to. The first domain you enter will become the default domain.

9. Click **Update** to save your changes.

### 7.6.3 Mapping PeopleSoft roles to Information platform services

Information platform services automatically creates a group for each PeopleSoft role that you map. As well, the program creates aliases to represent the members of the mapped PeopleSoft roles.

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in Information platform services.

Doing so reduces the number of accounts that are created for the same user in Information platform services.

For example, if you run PeopleSoft HR 8.3 and PeopleSoft Financials 8.4, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign

each user to an alias with the same name, then 60 accounts are created for the 30 users in Information platform services.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

For example, if you run PeopleSoft HR 8.3 with a user account for Russell Aquino (user name "raquino"), and you run PeopleSoft Financials 8.4 with a user account for Raoul Aquino (user name "raquino"), then you need to create a separate account for each user's alias. Otherwise, the two users are added to the same Information platform services account; they will be able to log in to Information platform services with their own PeopleSoft credentials and have access to data from both PeopleSoft systems.

### 7.6.3.1 To map a PeopleSoft role to Information platform services

1. Log on as an administrator to the Central Management Console.
2. Click **Authentication**.
3. Double-click **PeopleSoft Enterprise for PeopleTools**.
4. From the **Roles** tab, in the PeopleSoft Enterprise Domains area, select the domain associated with the role you want to map to Information platform services.
5. Use one of the following options to select the roles you want to map:
  - In the PeopleSoft Enterprise Roles area, in the Search roles text box, enter the role you want to locate and map to Information platform services, and then click >.
  - From the "Available Roles" list box, select the role you want to map to Information platform services and click >

#### **Note:**

- When searching for a particular user or role, you can use the wild card %. For example, to search for all roles beginning with "A," type **A%**. Search is also case sensitive.
  - If you want to map a role from another domain, you must select the new domain from the list of available domains to match a role from a different domain.
6. To enforce group and user synchronization between Information platform services and PeopleSoft, check the **Force user synchronization** check box. To remove already imported PeopleSoft groups from Information platform services, leave the **Force user synchronization** check box unchecked.
  7. In the "New Alias Options" area, select one of the following options:
    - **Assign each added alias to an account with the same name**

Select this option if you run multiple PeopleSoft Enterprise systems with users who have accounts on more than one system (and no two users have the same user name for different systems).
    - **Create a new account for every added alias**

Select this option if you run only one PeopleSoft Enterprise, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.

8. In the **Update Options** area, select one of the following options:

- **New aliases will be added and new users will be created**

Select this option to create a new alias for every user that is mapped to Information platform services. New accounts are added for users without Information platform services accounts or for all users if you selected the Create a new account for every added alias option.

- **No new aliases will be added and new users will not be created**

Select this option if the role that you want to map contains many users, but only a few of them will use Information platform services. Enterprise does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to Information platform services for the first time. This is the default option.

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

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

- **New users are created as BI Viewer**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.

- **New users are created as BI Analyst** New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all applications workflows that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.

If your Information platform services license is not based on users roles, select one of the following options:

- **New users are created as named users.**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

- **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 Information platform services 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 Information platform services, a 100 user concurrent license could support 250, 500, or 700 users.

The roles that you selected now appear as groups in Information platform services.

### 7.6.3.2 Remapping consideration

If you add users to a role that has already been mapped to Information platform services, you need to remap the role to add the users to Information platform services. When you remap the role, the option to map users as either named users or concurrent users affects only the new users that you added to the role.

For example, you first map a role to Information platform services with the "New users are created as named users" option selected. Later, you add users to the same role and remap the role with the "New users are created as concurrent users" option selected.

In this situation, only the new users in the role are mapped to Information platform services as concurrent users; the users that were already mapped remain named users. The same condition applies if you first map users as concurrent users, and then you change the settings to remap new users as named users.

### 7.6.3.3 To unmap a role

1. Log on as an administrator to the Central Management Console.
2. Click **Authentication**.
3. Click **PeopleSoft Enterprise**.
4. Click **Roles**.
5. Select the role that you want to remove, and click **<**.
6. Click **Update**.

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

**Note:**

You can also delete individual accounts or remove users from roles before you map them to Information platform services to prevent specific users from logging on.

### 7.6.4 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your Information platform services user data, you can schedule regular user updates. These updates will automatically synchronize

your ERP and Information platform services users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- **Update roles only:** using this option will update only the links between the currently mapped roles that have been imported in Information platform services. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- **Update roles and aliases:** this option not only updates links between roles but will also create new user accounts in Information platform services for new user aliases added to the ERP system.

**Note:**

If you have not specified to automatically create user aliases for updates when you enabled authentication, no accounts will be created for new aliases.

### 7.6.4.1 To schedule user updates

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

1. Click the **User Update** tab.
2. Click **Schedule** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

**Tip:**

If you want to run an update immediately click **Update Now**.

**Tip:**

Use the "Update Roles Only" option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

The "Recurrence" dialog box is displayed.

3. Select an option from the "Run Object" list and provide all the requested scheduling information.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.

Recurrence pattern	Description
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

- Click **Schedule** after you have finished providing the scheduling information.

The date of the next scheduled role update is displayed in the **User Update** tab.

**Note:**

You can always cancel the next scheduled update by clicking **Cancel Scheduled Updates** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

## 7.6.5 Using the PeopleSoft Security Bridge

The Security Bridge feature of Information platform services allows you to import PeopleSoft EPM security settings to Information platform services.

The Security Bridge operates in two modes:

- Configuration mode

In configuration mode, the Security Bridge provides an interface that enables you to create a response file. This response file is what governs the behavior of the Security Bridge during execution mode.

- Execution mode

Based on the parameters that you define in the response file, the Security Bridge imports the security settings of dimension tables in PeopleSoft EPM to universes in Information platform services.

### 7.6.5.1 Importing security settings

To import the security settings, you must do the following tasks in order:

- Define the objects that the Security Bridge will manage.
- Create a response file.
- Run the Security Bridge application.

For information about managing security after you import the settings, see the [Managing security settings](#) section.

#### 7.6.5.1.1 Defining managed objects

Before you run the Security Bridge, it is important to determine the objects that are managed by the application. The Security Bridge manages one or more PeopleSoft roles, an Information platform services group, and one or more universes.

- Managed PeopleSoft roles

These are roles in your PeopleSoft system. Members of these roles work with PeopleSoft data through PeopleSoft EPM. You must choose the roles that include the members for whom you want to provide/update access privileges to the managed universes in Information platform services.

The access rights that are defined for the members of these roles are based on their rights in PeopleSoft EPM; the Security Bridge imports these security settings to Information platform services.

- Managed Information platform services group

When you run the Security Bridge, the program creates a user in Information platform services for each member of a managed PeopleSoft role.

The group in which the users are created is the managed Information platform services group. Members of this group are the users whose access rights to the managed universes are maintained by the Security Bridge. Because the users are created in one group, you can configure the Security Bridge not to update the security settings for certain users simply by removing users from the managed Information platform services group.

Before you run the Security Bridge, you must choose a group in Information platform services to be the location where the users are created. If you specify a group that does not exist, the Security Bridge will create the group in Information platform services.

- Managed universes

Managed universes are the universes to which the Security Bridge imports security settings from PeopleSoft EPM. From the universes that are stored in your Information platform services system,

you must choose which ones are to be managed by the Security Bridge. Members of managed PeopleSoft roles who are also members of the managed Information platform services group cannot access any data through these universes that they cannot access from PeopleSoft EPM.

#### 7.6.5.1.2 To create a response file

1. Go to the folder that you specified during the installation of the Security Bridge, and run the `crpsepmsecuritybridge.bat` (in Windows) and `crpsepmsecuritybridge.sh` (in Unix) file.

**Note:**

In Windows, by default, this location is `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`

The Security Bridge for PeopleSoft EPM dialog box appears.

2. Select **New** to create a response file, or select **Open** and click **Browse** to specify a response file that you want to modify. Select the language you want for the file.
3. Click **Next >>**.
4. Provide the locations of the **PeopleSoft EPM SDK** and the **Information platform services SDK**.

**Note:**

- The PeopleSoft EPM SDK is typically located on the PeopleSoft server at `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.
- The SAP BusinessObjects Enterprise SDK is typically located at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib`.

5. Click **Next >>**.

The dialog box prompts you for connection and driver information for the PeopleSoft database.

6. From the Database list, select the appropriate database type, and provide the information for the following fields:

Field	Description
Database	The name of the PeopleSoft database.
Host	The name of the server that hosts the database.
Port number	The port number for accessing the server.
Class location	The location of the class files for the database driver.
User name	Your user name.

Field	Description
Password	Your password.

7. Click **Next >>**.

The dialog box displays a list of all the classes that the Security Bridge will use to run. If necessary, you can add to or remove classes from the list.

8. Click **Next >>**.

The dialog box prompts you for connection information for Information platform services.

9. Provide the appropriate information for the following fields:

Field	Description
Server	The name of the server where the Central Management Server (CMS) is located.
User name	Your user name.
Password	Your password.
Authentication	Your authentication type.

10. Click **Next >>**.

11. Choose an Information platform services group, and click **Next >>**.

**Note:**

- The group that you specify in this field is where the Security Bridge creates users for the members of the managed PeopleSoft roles.
- If you specify a group that does not already exist, it will be created by the Security Bridge.

The dialog box displays a list of roles from your PeopleSoft system.

12. Select the **Imported** option for the roles that you want the Security Bridge to manage, and click **Next >>**.

**Note:**

The Security Bridge creates a user in the managed Information platform services group (which you specified in the previous step) for each member of the role(s) that you select.

The dialog box displays a list of universes in Information platform services .

13. Select the universe(s) to which you want the Security Bridge to import security settings, and click **Next >>**.
14. Specify a filename for the Security Bridge log file and a location where the log file will be saved. You can use the log file to determine whether or not the Security Bridge is successful in importing the security settings from PeopleSoft EPM.
15. Click **Next >>**.

The dialog box displays a preview of the response file that the Security Bridge will use during execution mode.

16. Click **Save**, and choose a location where you want to save the response file.
17. Click **Next >>**.

You have successfully created the response file for the Security Bridge.

18. Click **Exit**.

**Note:**

The response file is a Java property file that you can also create and/or modify manually. For more details, see the “PeopleSoft response file” section.

## 7.6.5.2 Applying the security settings

To apply the security settings, run the `crpsepmsecuritybridge.bat` (in Windows) or the `crpsempsecuritybridge.sh` file (in UNIX), and use the response file that you created as an argument. (For example, type `crpsepmsecuritybridge.bat` (Windows) or `crpsempsecuritybridge.sh` (unix) `myresponsefile.properties`.)

The Security Bridge application runs. It creates users in Information platform services for the members of the PeopleSoft roles that you specified in the response file and imports the security settings from PeopleSoft EPM to the appropriate universes.

### 7.6.5.2.1 Mapping considerations

During execution mode, the Security Bridge creates a user in Information platform services for each member of a managed PeopleSoft role.

The users are created to have only Enterprise authentication aliases, and Information platform services assigns random passwords to these users. As a result, the users cannot log on to Information platform services until the administrator manually reassigns new passwords or maps the role(s) to Information platform services through the PeopleSoft Security Plug-in to allow the users to log on by using their PeopleSoft credentials.

### 7.6.5.3 Managing security settings

You can manage the security settings that you applied by modifying the objects that are managed by the Security Bridge.

#### 7.6.5.3.1 Managed users

The Security Bridge manages users based on the following criteria:

- Whether or not the user is a member of a managed PeopleSoft role.
- Whether or not the user is a member of the managed Information platform services group.

If you want to enable a user to access PeopleSoft data through universes in Information platform services , ensure that the user is a member of both a managed PeopleSoft role and the managed Information platform services group.

- For members of managed PeopleSoft roles who do not have accounts in Information platform services , the Security Bridge creates accounts and assigns random passwords to them. The administrator must decide whether or not to reassign new passwords manually or map the roles to Information platform services through the PeopleSoft Security Plug-in to allow the users to log on to Information platform services.
- For members of managed PeopleSoft roles who are also members of the managed Information platform services group, the Security Bridge updates the security settings that are applied to the users so that they have access to the appropriate data from the managed universes.

If a member of a managed PeopleSoft role has an existing account in Information platform services , but he/she is not a member of the managed Information platform services group, then the Security Bridge does not update the security settings that are applied to the user. Typically, this situation occurs only when the administrator manually removes user accounts that have been created by the Security Bridge from the managed Information platform services group.

**Note:**

This is an effective method for managing security: by removing users from the managed Information platform services group, you can configure their security settings to be different from the security settings that they have in PeopleSoft.

Conversely, if a member of the managed Information platform services group is not a member of a managed PeopleSoft role, then the Security Bridge does not provide them with access to the managed universes. Typically, this situation occurs only when PeopleSoft administrators remove users who have been previously mapped to Information platform services by the Security Bridge from the managed PeopleSoft role(s).

**Note:**

This is another method for managing security: by removing users from managed PeopleSoft roles, you can ensure that the users have no access to data from PeopleSoft.

### 7.6.5.3.2 Managed universes

The Security Bridge manages universes through restriction sets, which limit the data that managed users can access from the managed universes.

Restriction sets are groups of restrictions (for example, restrictions to Query Controls, SQL Generation, and so on). The Security Bridge applies/updates Row Access and Object Access restrictions for the managed universes:

- It applies Row Access restrictions to dimension tables that are defined in PeopleSoft EPM. These restrictions are user-specific and can be configured to one of the following settings:
  - The user has access to all of the data.
  - The user has access to none of the data.
  - The user has access to data based on their row-level permissions in PeopleSoft, which are exposed through the Security Join Tables (SJT) that are defined in PeopleSoft EPM.
- It applies Object Access restrictions to measure objects based on the fields that are accessed by the measure objects.

If a measure object accesses fields that are defined as metrics in PeopleSoft, then access to the measure object is allowed/disallowed depending on whether or not the user can access the referenced metrics in PeopleSoft. If a user cannot access any of the metrics, then access to the measure object is denied. If the user can access all of the metrics, then access to the measure object is granted.

As an administrator, you can also limit the data that users can access from your PeopleSoft system by limiting the number of universes that are managed by the Security Bridge.

### 7.6.5.4 PeopleSoft response file

The Security Bridge feature of Information platform services operates based on the settings that you specify in a response file.

Typically, you generate the response file by using the interface that is provided by the Security Bridge in configuration mode. However, because the file is a Java property file, you can also create or modify it manually.

This appendix provides information about the parameters that you need to include in the response file if you choose to generate it manually.

**Note:**

When you create the file, you must respect the Java property file escaping requirement (for example, ':' is escaped as '\:').

#### 7.6.5.4.1 Response file parameters

The following table describes the parameters that are included in the response file:

Parameter	Description
classpath	<p>The class path for loading the necessary .jar files. Multiple class paths must be separated by a ';' on both Windows and UNIX.</p> <p>The class paths that are needed are for the <code>com.peoplesoft.epm.pf.jar</code> and the JDBC driver .jar files.</p>
db.driver.name	<p>The JDBC driver name that is used to connect to the PeopleSoft database (for example, <code>com.microsoft.jdbc.sqlserver.SQLServerDriver</code>).</p>
db.connect.str	<p>The JDBC connection string that is used to connect to the PeopleSoft database (for example, <code>jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO</code>)</p>
db.user.name	<p>The user name for logging on to the PeopleSoft database.</p>
db.password	<p>The password for logging on to the PeopleSoft database.</p>
db.password.encrypted	<p>The value for this parameter determines whether the password parameter in the response file is encrypted or not. The value can be set to either True or False. (If no value is specified, the value becomes False by default.)</p>
enterprise.cms.name	<p>The CMS in which the universes are located.</p>
enterprise.user.name	<p>The user name for logging on to the CMS.</p>
enterprise.password	<p>The password for logging on to the CMS.</p>

Parameter	Description
enterprise.password.encrypted	The value for this parameter determines whether the password parameter in the response file is encrypted or not. The value can be set to either True or False. (If no value is specified, the value becomes False by default.)
enterprise.authMethod	The authentication method for logging on to the CMS.
enterprise.role	The managed Information platform services group.
enterprise.license	Controls the license type when importing users from PeopleSoft. "0" sets the named user license, "1" sets the concurrent user license.
peoplesoft.role.n	<p>The list of managed PeopleSoft roles.</p> <p><i>n</i> is an integer, and each entry occupies a property with the peoplesoft.role prefix.</p> <p><b>Note:</b> <i>n</i> is 1 based.</p> <p>You can use '*' to denote all available PeopleSoft roles, given that <i>n</i> is 1, and it is the only property that has peoplesoft.role as the prefix in the response file.</p>
mapped.universe.n	<p>The list of universes that you want the Security Bridge to update.</p> <p><i>n</i> is an integer, and each entry occupies a property with the mapped.universe prefix.</p> <p><b>Note:</b> <i>n</i> is 1 based.</p> <p>You can use '*' to denote all available universes, given that <i>n</i> is 1, and it is the only property that has mapped.universe as the prefix in the response file.</p>

Parameter	Description
log4j.appender.file.File	The log file that is written by the Security Bridge.
log4j.*	<p>Default log4j properties that are required for log4j to function properly:</p> <p>log4j.rootLogger=INFO, file, stdout</p> <p>log4j.appender.file=org.apache.log4j.RollingFileAppender</p> <p>log4j.appender.file.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.file.MaxFileSize=5000KB</p> <p>log4j.appender.file.MaxBackupIndex=100</p> <p>log4j.appender.file.layout.ConversionPattern=%d [ %-5 ] %c{1} - %m%n</p> <p>log4j.appender.stdout=org.apache.log4j.ConsoleAppender</p> <p>log4j.appender.stdout.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.stdout.layout.ConversionPattern=%d [ %-5 ] %c{1} - %m%n</p>
peoplesoft classpath	<p>The class path to the PeopleSoft EPM API .jar files.</p> <p>This parameter is optional.</p>
enterprise.classpath	<p>The class path to the Information platform services SDK .jar files.</p> <p>This parameter is optional.</p>

Parameter	Description
db.driver.type	<p>The PeopleSoft database type. This parameter can have one of the following values:</p> <p>Microsoft SQL Server 2000</p> <p>Oracle Database 10.1</p> <p>DB2 UDB 8.2 Fixpack 7</p> <p>Custom</p> <p>Custom may be used to specify databases other than the recognized types or versions.</p> <p>This parameter is optional.</p>
sql.db.class.location sql.db.host sql.db.port sql.db.database	<p>The location of the SQL Server JDBC driver .jar files, the SQL Server host machine, the SQL Server port, and the SQL Server database name.</p> <p>These parameter can be used only if the db.driver.type is Microsoft SQL Server 2000.</p> <p>These parameters are optional.</p>
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	<p>The location of the Oracle JDBC driver .jar files, the Oracle database host machine, the Oracle database port, and the Oracle database SID.</p> <p>These parameters can be used only if the db.driver.type is Oracle Database 10.1.</p> <p>These parameters are optional.</p>
db2.db.class.location db2.db.host db2.db.port db2.db.sid	<p>The location of the DB2 JDBC driver .jar files, the DB2 database host machine, the DB2 database port, and the DB2 database SID.</p> <p>These parameters can be used only if the db.driver.type is DB2 UDB 8.2 Fixpack 7</p> <p>These parameters are optional.</p>

Parameter	Description
custom.db.class.location	The location, name, and connection string of the custom JDBC driver.
custom.db.drivertype	These parameters can be used only if the db.driver.type is Custom.
custom.db.connectStr	
	These parameters are optional.

## 7.7 JD Edwards authentication

### 7.7.1 Overview

To use your JD Edwards data with Information platform services, you must provide the system with information about your JD Edwards deployment. This information is what allows Information platform services to authenticate users so that they can use their JD Edwards EnterpriseOne credentials to log on to Information platform services.

### 7.7.2 Enabling JD Edwards EnterpriseOne authentication

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

#### 7.7.2.1 To enable JD Edwards authentication in Information platform services

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click **Authentication**.
3. Double-click **JD Edwards EnterpriseOne**.

The "JD Edwards EnterpriseOne" page appears. It has four tabs: **Options**, **Servers**, **Roles**, and **User Update**.

4. On the **Options** tab, click **Enable JD Edwards EnterpriseOne Authentication** check box.
5. Make appropriate changes under **New Alias**, **Update Options**, and **New User Options** according to your Information platform services deployment. Click **Update** to save your changes before proceeding to the **Systems** tab.
6. Click the **Servers** tab.
7. In the "JD Edwards EnterpriseOne System User" area, type a database User name and Password for Information platform services to use to log on to your JD Edwards EnterpriseOne database.
8. In the "JD Edwards EnterpriseOne Domain" area, enter the name, host, and port used to connect to your JD Edwards EnterpriseOne environment, enter a name for the environment and click **Add**.
9. Click **Update** to save your changes.

### 7.7.3 Mapping JD Edwards EnterpriseOne roles to Information platform services

Information platform services automatically creates a group for each JD Edwards EnterpriseOne role that you map. As well, the system creates aliases to represent the members of the mapped JD Edwards EnterpriseOne roles.

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in Information platform services.

Doing so reduces the number of accounts that are created for the same user in Information platform services.

For example, if you run a JD Edwards EnterpriseOne test environment and production environment, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in Information platform services.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

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

### 7.7.3.1 To map a JD Edwards EnterpriseOne role to Information platform services

1. Log on as an administrator to the Central Management Console.
2. From the "Manage" area, click **Authentication**.
3. Double-click **JD Edwards EnterpriseOne**.
4. In the **New Alias Options** area, select one of the following options:
  - **Assign each added alias to an account with the same name**

Select this option if you run multiple JD Edwards EnterpriseOne Enterprise systems with users who have accounts on more than one system (and no two users have the same user name for different systems).
  - **Create a new account for every added alias**

Select this option if you run only one JD Edwards EnterpriseOne, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.
5. In the **Update Options** area, select one of the following options:
  - **New aliases will be added and new users will be created**

Select this option to create a new alias for every user that is mapped to Information platform services. New accounts are added for users without Information platform services accounts or for all users if you selected the Create a new account for every added alias option.
  - **No new aliases will be added and new users will not be created**

Select this option if the role that you want to map contains many users, but only a few of them will use Information platform services. Information platform services does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to Information platform services for the first time. This is the default option.
6. In the **New User Options** area specify how new users are created..

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

  - **New users are created as BI Viewer**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.
  - **New users are created as BI Analyst**

New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all applications workflows that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.

If your Information platform services license is not based on users roles, select one of the following options:

- **New users are created as named users.**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

- **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 Information platform services 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 Information platform services, a 100 user concurrent license could support 250, 500, or 700 users.

The roles that you selected now appear as groups in Information platform services.

7. Click the **Roles** tab.
8. Under **Select a Server**, select the JD Edwards server that contains the roles you want to map.
9. Under "Imported Roles", select the roles you want to map to Information platform services and click **<**.
10. Click **Update**.

The roles will be mapped to Information platform services.

### **7.7.3.2 Remapping consideration**

If you add users to a role that has already been mapped to Information platform services, you need to remap the role to add the users to Information platform services. When you remap the role, the option to map users as either named users or concurrent users affects only the new users that you added to the role.

For example, you first map a role to Information platform services with the "New users are created as named users" option selected. Later, you add users to the same role and remap the role with the "New users are created as concurrent users" option selected.

In this situation, only the new users in the role are mapped to Information platform services as concurrent users; the users that were already mapped remain named users. The same condition applies if you

first map users as concurrent users, and then you change the settings to remap new users as named users.

### 7.7.3.3 To unmap a role

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

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

**Note:**

You can also delete individual accounts or remove users from roles before you map them to Information platform services to prevent specific users from logging on.

### 7.7.4 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your Information platform services user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and Information platform services users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- Update roles only: using this option will update only the links between the currently mapped roles that have been imported in Information platform services. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in Information platform services for new user aliases added to the ERP system.

**Note:**

If you have not specified to automatically create user aliases for updates when you enabled authentication, no accounts will be created for new aliases.

### 7.7.4.1 To schedule user updates

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

1. Click the **User Update** tab.
2. Click **Schedule** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

**Tip:**

If you want to run an update immediately click **Update Now**.

**Tip:**

Use the "Update Roles Only" option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

The "Recurrence" dialog box is displayed.

3. Select an option from the "Run Object" list and provide all the requested scheduling information.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.

Recurrence pattern	Description
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

- Click **Schedule** after you have finished providing the scheduling information.  
The date of the next scheduled role update is displayed in the **User Update** tab.

**Note:**

You can always cancel the next scheduled update by clicking **Cancel Scheduled Updates** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

## 7.8 Siebel authentication

### 7.8.1 Enabling Siebel authentication

To allow Siebel information to be used by Information platform services, Enterprise needs information on how to authenticate into your Siebel system.

#### 7.8.1.1 To enable Siebel authentication in Information platform services

- Log on as an administrator to the Central Management Console.
- From the Manage area, click **Authentication**.
- Double-click **Siebel**.  
The "Siebel" page appears. It has four tabs: **Options**, **Systems**, **Responsibilities**, and **User Update**.
- On the **Options** tab, select the **Enable Siebel Authentication** check box.
- Make appropriate changes under **New Alias**, **Update Options**, and **New User Options** according to your Information platform services deployment. Click **Update** to save your changes before proceeding to the **Systems** tab.
- Click the **Domains** tab.

7. In the **Domain Name** field enter the domain name for the Siebel system you want to connect to.
8. Under **Connection** enter the connection string for that domain.
9. In the **Username** area, type a database User name and Password for Information platform services to use to log on to your Siebel database.
10. In the **Password** area, enter the password for the user you have selected.
11. Click **Add** to add the system information to your "Current Domains" list.
12. Click **Update** to save your changes.

## 7.8.2 Mapping roles to Information platform services

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

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in Information platform services.

Doing so reduces the number of accounts that are created for the same user in the program.

For example, if you run a Siebel eBusiness test environment and production environment, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in Information platform services.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

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

### 7.8.2.1 To map a Siebel eBusiness role to Information platform services

1. Log on as an administrator to the Central Management Console.
2. Click **Authentication**.
3. Double-click **Siebel eBusiness**.
4. In the **New Alias Options** area, select one of the following options:

- **Assign each added alias to an account with the same name**

Select this option if you run multiple Siebel eBusiness systems with users who have accounts on more than one system (and no two users have the same user name for different systems).

- **Create a new account for every added alias**

Select this option if you run only one Siebel eBusiness, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.

5. In the **Update Options** area, select one of the following options:

- **New aliases will be added and new users will be created**

Select this option to create a new alias for every user that is mapped to Information platform services. New accounts are added for users without Information platform services accounts or for all users if you selected the Create a new account for every added alias option.

- **No new aliases will be added and new users will not be created**

Select this option if the role that you want to map contains many users, but only a few of them will use Information platform services. The program does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to Information platform services for the first time. This is the default option.

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

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

- **New users are created as BI Viewer**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.

- **New users are created as BI Analyst**

New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all applications workflows that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.

If your Information platform services license is not based on users roles, select one of the following options:

- **New users are created as named users.**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many

other people are connected. You must have a named user license available for each user account created using this option.

- **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 Information platform services 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 Information platform services, a 100 user concurrent license could support 250, 500, or 700 users.

7. Click the **Roles** tab.

8. Select the domain that corresponds to the Siebel server you want to map roles for.

9. Under "Available roles", select the roles you want to map and click >.

**Note:**

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

10. Click **Update**.

The roles will be mapped to Information platform services.

### 7.8.2.2 Remapping consideration

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

**Note:**

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

When you remap the role, the option to map users as either named users or concurrent users affects only the new users that you added to the role.

For example, you first map a role to Information platform services with the "New users are created as named users" option selected. Later, you add users to the same role and remap the role with the "New users are created as concurrent users" option selected.

In this situation, only the new users in the role are mapped to Information platform services as concurrent users; the users that were already mapped remain named users. The same condition applies if you first map users as concurrent users, and then you change the settings to remap new users as named users.

### 7.8.2.3 To unmap a role

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

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

**Note:**

You can also delete individual accounts or remove users from roles before you map them to Information platform services to prevent specific users from logging on.

### 7.8.3 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your Information platform services user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and Information platform services users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- Update roles only: using this option will update only the links between the currently mapped roles that have been imported in Information platform services. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in Information platform services for new user aliases added to the ERP system.

**Note:**

If you have not specified to automatically create user aliases for updates when you enabled authentication, no accounts will be created for new aliases.

### 7.8.3.1 To schedule user updates

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

1. Click the **User Update** tab.
2. Click **Schedule** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

**Tip:**

If you want to run an update immediately click **Update Now**.

**Tip:**

Use the "Update Roles Only" option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

The "Recurrence" dialog box is displayed.

3. Select an option from the "Run Object" list and provide all the requested scheduling information.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.

Recurrence pattern	Description
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click **Schedule** after you have finished providing the scheduling information.  
The date of the next scheduled role update is displayed in the **User Update** tab.

**Note:**

You can always cancel the next scheduled update by clicking **Cancel Scheduled Updates** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

## 7.9 Oracle EBS authentication

### 7.9.1 Enabling Oracle EBS authentication

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

#### 7.9.1.1 To enable Oracle E-Business Suite authentication

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click **Authentication**.
3. Click **Oracle EBS**.  
The "Oracle EBS" page appears. It has four tabs: **Options**, **Systems**, **Responsibilities**, and **User Update**.
4. On the **Options** tab, select the **Oracle EBS Authentication is enabled** check box.
5. Make appropriate changes under **New Alias**, **Update Options**, and **New User Options** according to your Information platform services deployment. Click **Update** to save your changes before proceeding to the **Systems** tab.

6. Click the **Systems** tab.
7. In the "Oracle EBS System User" area, type a database User name and Password for Information platform services to use to log on to your Oracle E-Business Suite database.
8. In the "Oracle EBS Services" area, enter the service name used by your Oracle EBS environment and click **Add**.
9. Click **Update** to save your changes.

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

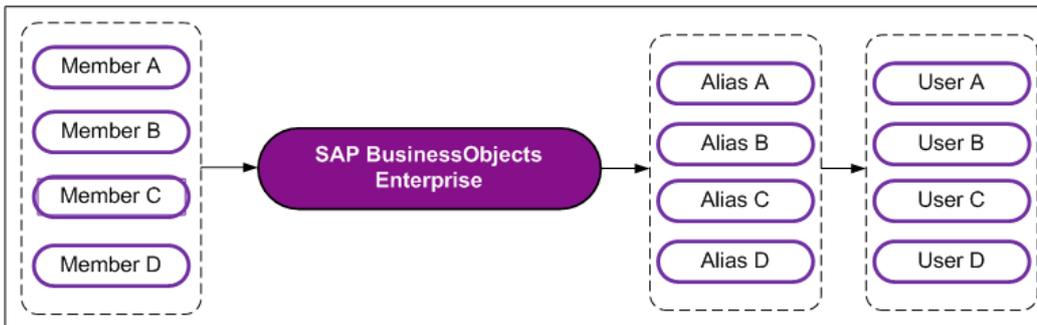
**Related Topics**

- [Mapping Oracle E-Business Suite roles to Information platform services](#)

## 7.9.2 Mapping Oracle E-Business Suite roles to Information platform services

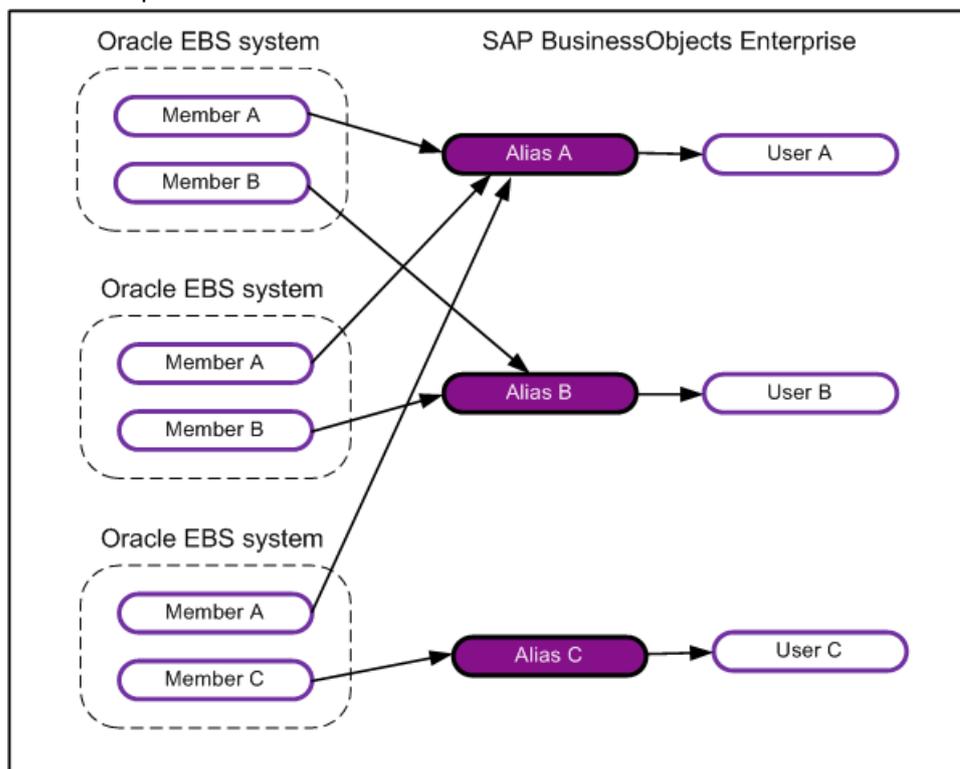
Information platform services automatically creates a group for each Oracle E-Business Suite (EBS) role that you map. Information platform services also creates aliases to represent the members of the mapped Oracle E-Business Suite roles.

You can create a user account for each alias that is created.



However, if you run multiple systems and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in

Information platform services.



Doing so reduces the number of accounts that are created for the same user in Information platform services.

For example, if you run a EBS test environment and production environment, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in Information platform services.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

For example, if you run your test environment with a user account for Russell Aquino (user name "raqino"), and you run the production environment with a user account for Raoul Aquino (user name "raqino"), then you need to create a separate account for each user's alias. Otherwise, the two users are added to the same Information platform services account; they will be able to log on to Information platform services with their own Oracle EBS credentials and have access to data from both EBS environments.

### 7.9.2.1 To map Oracle E-Business Suite roles to Information platform services

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click **Authentication**.
3. Click **Oracle EBS**.

The "Oracle EBS" page displays the **Options** tab.

4. In the "New Alias Options" area, select one of the following options:

- **Assign each added Oracle EBS alias to an account with the same name**

Select this option if you run multiple Oracle E-Business Suite systems with users who have accounts on more than one system (and if no two users have the same user name for different systems).

- **Create a new account for every added Oracle EBS alias**

Select this option if you run only one Oracle E-Business Suite, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.

5. In the "Update Options" area, select one of the following options:

- **New aliases will be added and new users will be created**

Select this option to create a new alias for every user that is mapped to Information platform services. New accounts are added for users without Information platform services accounts or for all users if you selected the **Create a new account for every added Oracle EBS alias** option.

- **No new aliases will be added and new users will not be created**

Select this option if the role that you want to map contains many users, but only a few of them will use Information platform services. Information platform services does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to Information platform services for the first time. This is the default option.

6. In "New User Options" specify how new users are created, and then click **Update**.

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

- **New users are created as BI Viewer**

New user accounts are configured under the BI Viewer role. Access to Information platform services applications for all accounts under the BI Viewer role is defined in the license agreement. Users are restricted to access application workflows that are defined for the BI Viewer role. Access rights are generally limited to viewing business intelligence documents. This role is typically suitable for users who consume content through Information platform services applications.

- **New users are created as BI Analyst**

New user accounts are configured under the BI Analyst role. Access to Information platform services applications for all accounts under the BI Analyst role is defined in the license agreement. Users can access all applications workflows that are defined for the BI Analyst role. Access rights include viewing and modifying business intelligence documents. This role is typically suitable for users who create and modify content for Information platform services applications.

If your Information platform services license is not based on users roles, select one of the following options:

- **New users are created as named users.**

New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.

- **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 Information platform services 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 Information platform services, a 100 user concurrent license could support 250, 500, or 700 users.

The roles that you selected now appear as groups in Information platform services.

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

11. Click **Update**.

The roles will be mapped to Information platform services.

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

### **Related Topics**

- [Role-based licensing](#)

#### 7.9.2.1.1 Updating Oracle EBS roles and users

After enabling Oracle EBS authentication, it is necessary to schedule and run regular updates on mapped roles that have been imported into Information platform services. This will ensure that updated Oracle EBS role information is accurately reflected in Information platform services.

There are two options for running and scheduling updates for Oracle EBS roles:

- Update roles only: using this option will only update the links between the currently mapped roles that have been imported in Information platform services. It is recommended that you use this option if you expect to run frequent updates, and you have concerns over system resource usage. No new user accounts will be created if you only update Oracle EBS roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in Information platform services for user aliases added to roles in the Oracle EBS system.

**Note:**

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

### 7.9.2.1.2 To schedule updates for Oracle EBS roles

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

1. Click the **User Update** tab.
2. Click **Schedule** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

**Tip:**

If you want to immediately run an update click **Update Now**.

**Tip:**

Use the "Update Roles Only" option if you would like frequent updates and have concerns about system resources. It takes the system longer to update both roles and aliases.

The "Recurrence" dialog box is displayed.

3. Select an option from the "Run Object" pull-down list and provide all the requested scheduling information in the fields provided.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.

Recurrence pattern	Description
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

- Click **Schedule** after you have finished providing the scheduling information.  
The date of the next scheduled role update is displayed in the **User Update** tab.

**Note:**

You can always cancel the next scheduled update by clicking **Cancel Scheduled Updates** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

## 7.9.3 Unmapping roles

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

### 7.9.3.1 To unmap a role

- Log on as an administrator to the Central Management Console.
- From the Manage area, click **Authentication**.
- Double-click the name of the ERP system you want to unmap roles for.  
The ERP system page displays the **Options** tab.
- Click the **Responsibilities** or **Roles** tab.

5. Select the target role from the **Mapped Roles** or **Imported Roles** area and click < or **Delete** to remove them.
6. Click **Update**.

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

**Note:**

You can also delete individual accounts or remove users from roles before you map them to Information platform services to prevent specific users from logging on.

## 7.9.4 Customizing rights for mapped Oracle EBS groups and users

When you map roles to Information platform services, you can set rights or grant permissions for the groups and users that are created.

### 7.9.4.1 To assign administration rights

To allow users to maintain Information platform services, you must make them members of the default Administrator's group. Members of this group receive full control over all aspects of Information platform services, which includes accounts, servers, folders, objects, settings, and so on.

1. Log on as an administrator to the Central Management Console.
2. From the "Organize" area, click **Users**.
3. In the **Name** column, click **Administrators**.
4. Click **Group List**, and then from the Actions list, click **Add**.

The Available Users/Groups page appears.

5. From the **User List** or **Group List** area, select the mapped role to which you want to assign administrative rights.
6. Click > to make the role a subgroup of the Administrators group, and click **OK**.

Members of the role now have administration rights in Information platform services.

**Note:**

You can also create a role within Oracle EBS, add the appropriate users to the role, map the role to Information platform services, and make the mapped role a subgroup of the default Administrator's group to grant members of the role administrative rights.

### 7.9.4.2 To assign publishing rights

If your system has users who are designated as content creators within your organization, you can grant them permission to publish objects to Information platform services.

1. Log on as an administrator to the Central Management Console.
2. From the "Organize" area, click **Folders**.
3. Go to the folder where you want to allow users to add objects.
4. Click **Manage, Top-Level Security** and then **All Folders**.
5. Click **Add Principals**.

The Add Principals page appears.

6. In the **Available users/groups** list, select the group that includes the members to whom you want to give publishing rights.
7. Click > to enable the group to access the folder, and then click **Add & Assign Security**.

The Assign Security page appears.

8. In the **Available Access Level** list, select the access level you want and click > to explicitly assign the access level.
9. If the **Inherit from Parent Folder** and **Inherit from Parent Group** options are selected, deselect them, and click **Apply**.
10. Click **OK**.

Members of the role now have permission to add objects to the folder and all of its subfolders. To remove assigned permissions, click **Remove Access**.

## 7.10 Automated user updates

### 7.10.1 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your Information platform services user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and Information platform services users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- **Update roles only:** using this option will update only the links between the currently mapped roles that have been imported in Information platform services. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- **Update roles and aliases:** this option not only updates links between roles but will also create new user accounts in Information platform services for new user aliases added to the ERP system.

**Note:**

If you have not specified to automatically create user aliases for updates when you enabled authentication, no accounts will be created for new aliases.

### 7.10.1.1 To schedule user updates

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

1. Click the **User Update** tab.
2. Click **Schedule** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

**Tip:**

If you want to run an update immediately click **Update Now**.

**Tip:**

Use the "Update Roles Only" option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

The "Recurrence" dialog box is displayed.

3. Select an option from the "Run Object" list and provide all the requested scheduling information.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.

Recurrence pattern	Description
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click **Schedule** after you have finished providing the scheduling information.  
The date of the next scheduled role update is displayed in the **User Update** tab.

**Note:**

You can always cancel the next scheduled update by clicking **Cancel Scheduled Updates** in either the "Update Roles Only" or "Update Roles and Aliases" sections.

# Server Administration

## 8.1 Server Administration

### 8.1.1 Working with the Servers management area in the CMC

The Servers management area of the CMC is your primary tool for server management tasks. It provides a list of all of the servers in your deployment. For most management and configuration tasks, you need to select a server in the list and choose a command from the Manage or Action menu.

#### About the navigation tree

The navigation tree on the left side of the Servers management area provides a number of ways to view the Servers list. Select items in the navigation tree to change the information displayed in the "Details" pane.

Navigation tree option	Description
<b>Servers List</b>	Displays a complete list of all servers in the deployment.
<b>Server Groups List</b>	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.
<b>Server Groups</b>	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.

Navigation tree option	Description
<b>Nodes</b>	Displays a list of the nodes in your deployment. Nodes are configured in the CCM. You can select a node by clicking it to view or manage the servers on the node.
<b>Service Categories</b>	<p>Provides a list of the types of services that may be in your deployment. Service categories are divided into core Information platform services and services associated with specific SAP Business Objects components. Service categories include:</p> <ul style="list-style-type: none"><li>• <b>Connectivity Services</b></li><li>• <b>Core Services</b></li><li>• <b>Crystal Reports Services</b></li><li>• <b>Data Federation Services</b></li><li>• <b>Lifecycle Management Services</b></li><li>• <b>Analysis Services</b></li><li>• <b>Web Intelligence Services</b></li><li>• <b>Dashboard Design Services</b></li></ul> <p>Select a service category in the navigation list to view or manage the servers in the category.</p> <p><b>Note:</b> A server may host services belonging to multiple service categories. Therefore a server can appear in several service categories.</p>

Navigation tree option	Description
<b>Server Status</b>	<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"> <li>• <b>Stopped</b></li> <li>• <b>Starting</b></li> <li>• <b>Initializing</b></li> <li>• <b>Running</b></li> <li>• <b>Stopping</b></li> <li>• <b>Started with Errors</b></li> <li>• <b>Failed</b></li> <li>• <b>Waiting for resources</b></li> </ul>

#### 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
<b>Server Name or Name</b>	Displays the name of the server.

Details pane column	Description
<b>State</b>	<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"> <li>• <b>Stopped</b></li> <li>• <b>Starting</b></li> <li>• <b>Initializing</b></li> <li>• <b>Running</b></li> <li>• <b>Stopping</b></li> <li>• <b>Started with Errors</b></li> <li>• <b>Failed</b></li> <li>• <b>Waiting for resources</b></li> </ul>
<b>Enabled</b>	Displays whether the server is enabled or disabled.
<b>Stale</b>	If the server is marked as <b>Stale</b> , then it requires a restart. For example, if you change certain server settings in the server's "Properties" screen, you may need to restart the server before the changes will take effect.
<b>Kind</b>	Displays the type of server.
<b>Host Name</b>	Displays the Host Name for the server.
<b>Health</b>	Indicates the general health of the server.
<b>PID</b>	Displays the unique Process ID number for the server.
<b>Description</b>	Displays a description of the server. You can change this description in the server's "Properties" page.
<b>Date Modified</b>	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.

**Related Topics**

- [Managing server groups](#)
- [Using nodes](#)
- [Viewing the state of servers](#)
- [To start, stop, or restart servers with CMC](#)
- [To change a server's properties](#)

## 8.1.2 Managing servers by using scripts on Windows

The `ccm.exe` executable lets you start, stop, restart, enable, and disable the servers in your Windows deployment through the command line.

## 8.1.3 Managing servers on Unix

The `ccm.sh` executable lets you start, stop, restart, enable, and disable the servers in your Unix deployment through the command line.

## 8.1.4 Managing License keys

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

**Related Topics**

- [To add a license key](#)
- [To view license information](#)
- [To view current account activity](#)

### 8.1.4.1 To view license information

The **License Keys** management area of the CMC identifies the number of role-based (BI Viewer and BI Analyst), concurrent, named, and processor licenses that are associated with each key.

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

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

#### **Related Topics**

- [Managing License keys](#)
- [To add a license key](#)
- [To view license information](#)

### **8.1.4.2 To add a license key**

If you are upgrading from a trial version of the product, be sure to delete the Evaluation key prior to adding any new license keys or product activation keycodes.

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

The key is added to the list.

#### **Related Topics**

- [To add a license key](#)
- [To view current account activity](#)

### **8.1.4.3 To view current account activity**

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

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

#### **Related Topics**

- [Managing License keys](#)
- [To add a license key](#)
- [To view license information](#)

## 8.1.5 Measuring licenses

The BusinessObjects License Measurement Tool (BOLMT) is a java command-line utility used to collect and store Information platform services licensing data. The output XML document contains license deployment measurements and is sent to SAP Global License Auditing Services (GLAS) for consolidation as part of a license audit.

The system administrator installs and runs BOLMT for every Information platform services cluster whenever a license audit is requested. BOLMT collects usage measurements on role-based, named, and concurrent user licenses.

The administrator can specify a particular output directory for the XML document, and configure the output document to not contain any information that may be used to identify system users.

### 8.1.5.1 To run a license audit

To perform a license audit, you will need administrator rights and access to the directory containing the `BOLMT.jar` file in the Information platform services installation.

1. Open a command line console.
2. Change directories to the directory containing the java executables for your Information platform services installation

By default the file is installed in the `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib` directory.

3. Execute the `BOLMT.jar`.

The execution command is entered in the following format: `-jar BOLMT.jar [options] <outputFile>`

The table below summarizes the available options:

Option	Description
-c --cms	Specifies the name identifier and port number for the Central Management Server (CMS). Specified as <i>cmsname:port number</i> . By default, the CMS settings for the local host are used if this setting is not specified.
-p --password	Specifies the administrator account password used to connect to the CMS.
-a--auth	Specifies the authentication method to connect user to the CMS. Default method is Enterprise specified as <i>secEnterprise</i> .
-s--sanitize	Specifies that the output audit document should filter out any personal information that may be used to identify users.

**Note:**

The output file specification is always the last argument in the command line. It is an optional setting. If no argument is specified, the output goes to the console's standard output. You can also pipe output to script as a command line argument.

**Example:**

```
C:\Program Files (x86)\SAP
Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\lib>"C:\Program Files
(x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
\java.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```

## 8.1.6 Viewing and changing a server's status

### 8.1.6.1 Viewing the state of servers

The status of a server is its current state of operation: a server can be running, starting, stopping, stopped, failed, initializing, started with errors, or waiting for resources. To respond to Information platform services 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 Information platform services. A server that is stopped is no longer running as a process.

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

**Related Topics**

- [Viewing the state of servers](#)
- [Starting, stopping, and restarting servers](#)

- [Enabling and disabling servers](#)
- [Stopping a Central Management Server](#)
- [To start a server automatically](#)

#### 8.1.6.1.1 To view a server's status

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

The "Details" pane displays the service categories in your deployment.

2. To view a list of servers in a given Server Group, Node, or Service Category, in the navigation tree click the server group, node, or category.

The "Details" pane displays the list of servers in your deployment. A **State** column that provides the status for each server in the list.

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

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

**Note:**

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

### 8.1.6.2 Starting, stopping, and restarting servers

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

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

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

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

**Tip:**

When you stop (or restart) a server, you terminate the server's process, thereby stopping the server completely. Before you stop a server, it is recommended that you

- Disable the server so it can finish processing any jobs it has in progress, and
- Ensure that there are no auditing events remaining in the queue. To view the number of auditing events remaining in the queue, navigate to the server's "Metrics" window and view the **Current Number of Auditing Events in the Queue** value.

**Related Topics**

- [Enabling and disabling servers](#)

**8.1.6.2.1 To start, stop, or restart servers with CMC**

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

The "Details" pane displays the service categories in your deployment.

2. To view a list of servers in a particular Server Group, Node, or Service Category, select the group, node, or category on the navigation pane.

The "Details" pane displays a list of servers.

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

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

**Note:**

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

4. Right-click the server whose status you want to change, and depending on the action you need to perform select **Start Server**, **Restart Server**, **Stop Server**, or **Force Termination**.

**Related Topics**

- [Viewing the state of servers](#)

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

1. In the CCM, click the **Manage Servers** button on the toolbar.
2. When prompted, log on to your CMS with an administrative account.
3. In the "Manage Servers" dialog box, select the server that you want to start, stop, or restart.
4. Click **Start**, **Stop**, **Restart**, or **Force Terminate**.
5. Click **Close** to return to the CCM.

#### 8.1.6.2.3 To start a server automatically

You can set servers in your deployment to start automatically, by default, when the Server Intelligence Agent (SIA) starts.

1. In the "Servers" management area of the CMC, double-click the server that you want to start automatically.  
The "Properties" page appears.
2. Under "Common Settings", select the **Automatically start this server when the Server Intelligence Agent starts** check box, and click **Save** or **Save & Close**.

**Note:**

If the **Automatically start this server when the Server Intelligence Agent starts** check box is cleared for each CMS in the cluster, you must use the CCM to restart the system. After using the CCM to stop the SIA, right-click the SIA and click **Properties**. On the **Startup** tab, set **Autostart** to **Yes**, and click **Save**. Restart the SIA. The **Autostart** option is available only when the **Automatically start this server when the Server Intelligence Agent starts** check box is cleared for all CMSs in the cluster.

### 8.1.6.3 Stopping a Central Management Server

If your Information platform services 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 Information platform services out of service.

However, if your Information platform services deployment has a single CMS, shutting it down will make Information platform services 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 Information platform services shuts down, because all other servers on the node will also shut down.

**Note:**

When the CMS has been stopped, you may need to restart the system from the CCM. For example, if you shut down all CMSs on a node and the CMSs are not set to automatically start when the SIA starts, you must use the CCM to restart the system. In the CCM, right-click the SIA and click **Properties**. On the **Startup** tab, set **Autostart** to **Yes**, and click **Save**. Restart the SIA. The **Autostart** option is available only when the **Automatically start this server when the Server Intelligence Agent starts** check box is cleared for each CMS in the cluster.

If you want to configure your system so that you can start and stop the CMS in the cluster without starting and stopping other servers, put the CMS on a separate node. Create a new node and clone the CMS to the node. With the CMS on its own node, you can easily shut down the node without affecting other servers.

**Related Topics**

- [Using nodes](#)
- [Cloning servers](#)
- [Clustering Central Management Servers](#)

### 8.1.6.4 Enabling and disabling servers

When you disable an Information platform services server, you prevent it from receiving and responding to new Information platform services requests, but you do not actually stop the server process. This is useful when you want to allow a server to finish processing all of its current requests before you stop it completely.

For example, you may want to stop a Job Server before rebooting the machine it is running on. However, you want to allow the server to fulfill any outstanding report requests that are in its queue. First, you disable the Job Server so it cannot accept any additional requests. Next, go to the Central Management Console to monitor when the server completes the jobs it has in progress. (From the "Servers"

management area, right-click the server and select "Metrics".) Then, once it has finished processing current requests, you can safely stop the server.

**Note:**

- The CMS must be running in order for you to enable and/or disable other servers.
- A CMS cannot be enabled or disabled.

#### 8.1.6.4.1 To enable and disable servers with CMC

1. Go to the "Servers" management area of the CMC.
2. Right-click the server whose status you want to change, and depending on the action you need to perform click **Enable Server** or **Disable Server**.

#### 8.1.6.4.2 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 Information platform services.
3. In the "Manage Servers" dialog box, select the server that you want to enable or disable.
4. Click **Enable** or **Disable**.
5. Click **Close** to return to the CCM.

## 8.1.7 Adding, cloning, or deleting servers

### 8.1.7.1 Adding, cloning, and deleting servers

If you want to add new hardware to Information platform services by installing server components on new, additional machines, run the Information platform services installation program from your product distribution. The setup program allows you to perform a Custom installation. During the Custom installation, specify the CMS from your existing deployment, and select the components that you want to install on the local machine. For details on custom installation options, see the *Information platform services Installation Guide*.

#### 8.1.7.1.1 Adding a server

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

1. Go to the "Servers" management area of the CMC.
2. On the **Manage** menu, click **New > New Server**.

The "Create New Server" dialog box appears.

3. Choose the **Service Category**.
4. Choose the type of service that you need from the **Select Service** list, then click **Next**.
5. To add an additional service to the server, select the service in the **Available Additional Services** list and click **>**.

**Note:**

Additional services are not available for all server types.

6. After adding the additional services you want, click **Next**.
7. If your Information platform services 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 *<NODE NAME>.<servertype>* (a number is appended if there is more than one server of the same type on the same host machine).

9. To include a description for the server, type it into the **Description** box.
10. If you are adding a new Central Management Server, specify a port number in the **Name Server Port** field.
11. Click **Create**.  
The new server appears in the list of servers in the **Servers** area of the CMC, but it is neither started nor enabled.
12. Use the CMC to start and enable the new server when you want it to begin responding to Information platform services requests.

**Related Topics**

- [Services and servers](#)
- [Configuring server settings](#)
- [Configuring port numbers](#)
- [Viewing the state of servers](#)

#### 8.1.7.1.2 Cloning servers

If you want to add a new server instance to your deployment, you can clone an existing server. The cloned server retains the configuration settings of the original server. 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 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 to the same machine, 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 Information platform services (and any updates, if applicable).
- You can clone servers from any machine. However, you can only clone servers 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*

Placeholders are node-level variables that are used by servers running on the node; they are listed on a page in the Central Management Console (CMC). When you double-click a server listed under "Servers" in the CMC, a link appears on the left navigation pane for "Placeholders". The "Placeholders" page lists the available placeholder names and associated values for the selected server. Placeholders contain read-only values, and placeholder names begin and end with the percent sign (%).

**Tip:**

You can overwrite a placeholder setting with a specific string on the CMC Server "Properties" page.

**Example:**

Placeholders are useful when cloning servers. On multi-drive computer A, SAP BusinessObjects Enterprise is installed at `D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. The `%DefaultAuditingDir%` placeholder will be `D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

On another computer B, there is only one disc drive (no drive D:) and SAP BusinessObjects Enterprise is installed at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. The `%DefaultAuditingDir%` placeholder will be `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

To clone the Event Server from computer A to computer B, if you enter a placeholder for the **Auditing Temporary Directory** value, the placeholder will resolve itself and the Event Server will work properly. If no placeholder is used, the Event Server will fail, unless you manually overwrite the **Auditing Temporary Directory** value.

---

### *To clone a server*

1. On the machine that you want to add the cloned server to, go to the "Servers" management area of the CMC.
2. Right-click the server that you want to clone and select **Clone Server** .  
The "Clone Server" dialog box appears.

3. Type a name for the server (or use the default name) in the **New Server Name** field.
4. If you are cloning a Central Management Server, specify a port number in the **Name Server Port** field.
5. On the **Clone to Node** list, choose the node where you want to add the cloned server, then click **OK**.

The new server appears in the "Servers" management area of the CMC.

**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.

#### 8.1.7.1.3 Deleting a server

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

## 8.1.8 Clustering Central Management Servers

### 8.1.8.1 Clustering Central Management Servers

If you have a large or mission-critical implementation of SAP BusinessObjects Business Intelligence platform, you may need to run several CMS computers together in a cluster. A cluster consists of two or more CMS servers working together against a common CMS system database. If a computer that is running one CMS fails, a computer with another CMS will continue to service Business Intelligence platform requests. This high-availability support helps to ensure that Business Intelligence platform users can 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 computers. For information about the current CMS, go to the "Servers" management area of the CMC.

Before clustering CMS computers, make sure that each CMS is installed on an operating system that meets the requirements (including version level and patch level) outlined in the Product Availability Matrix for database servers, database access methods, database drivers, and database clients. 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, Business Intelligence platform performance will be greatly affected.
- For best performance, run each CMS cluster member on a computer that has the same amount of memory and the same type of CPU.
- Configure each computer similarly:
  - Install the same operating system, including the same version of operating system service packs and patches.
  - Install the same version of Business Intelligence platform (including patches, if applicable).
  - Ensure that each CMS connects to the CMS system database in the same manner: whether you use native or ODBC drivers. Make sure that the drivers are the same on each computer, 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 computer (including settings for daylight savings time).
  - Ensure that the same WAR files are installed on all web application servers in the cluster. For information about WAR file deployment, see the *Business Intelligence Platform Services Installation Guide*.
- Ensure that each CMS in a cluster is on the same Local Area Network.
- If a 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 information about server command lines in the *Business Intelligence Platform Services Administrator's Guide*.
- The Out-of-Band threads (`-oobthreads`) are used by clustering pings and clustering notifications. Both operations are very quick (notifications were changed to be asynchronous) so the need for many `oobthreads` has decreased. As a result, the value for this parameter is irrelevant, and only one `oobthread` is created.
- 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 computer hostname of the first CMS that you install.

**Related Topics**

- [Changing the name of a CMS cluster](#)

#### 8.1.8.1.1 Adding a CMS to a cluster

There are several ways to add a new CMS cluster member:

- You can install a new node with a CMS on a new computer.
- If you already have a node with CMS binary files, you can add a new CMS server from the CMC.
- If you already have a node with CMS binary files, you can also add a new CMS server by cloning an existing CMS server.

**Note:**

Back up your current CMS system database, server configuration, and the contents of your Input File Repository and Output File Repository before making any changes. If necessary, contact your database administrator.

**Related Topics**

- [Adding a new node to a cluster](#)
- [Adding a server](#)
- [To clone a server](#)

#### 8.1.8.1.2 Adding a new node to a cluster

When you add a node, you are prompted to either create a new CMS or to cluster the node to an existing CMS.

If you want to cluster a node to an existing CMS, you can also use the installation setup program. Run the Information platform services installation and setup program on the computer 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 computer. In this case, specify the name of the CMS that is running your existing system, and choose to install a new CMS on the local computer. 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 computer, it automatically adds the server to your existing cluster.

**Related Topics**

- [Using nodes](#)

#### 8.1.8.1.3 Adding clusters to the web application property files

If you have added additional CMSs to your deployment, and you are using a Java application server, you must modify the `PlatformServices.properties` file in the `\webapps\BOE\WEB-INF\config\custom` directory of your web application deployment.

*To define cluster properties for the BOE web application*

1. Access the custom folder for the `BOE.war` file on the computer hosting the web applications.

If you are using the Tomcat web application server installed with SAP BusinessObjects Business Intelligence platform, you can access the following folder:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
```

**Tip:**

If you are using a web application server that does not enable direct access to the deployed web applications, you can use the following folder in your product installation to modify the `BOE.war` file.

```
<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

You will have to later redeploy the modified `BOE.war` file.

2. Create a new file.

Use Notepad or any other text editing utility.

3. Specify CMC cluster properties for each cluster in your deployment.

Precede each cluster name with an `@` symbol, and 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 it is specified.

Use the `cms.clusters` property to specify each cluster in your deployment. For example, `cms.clusters=@samplecluster,@samplecluster2, @samplecluster3`. Use the `cms.clusters.[cluster name]` property to specify each CMS in the cluster. For example:

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400,cmstwo
cms.clusters.samplecluster2=cms3,cms4, cms5
cms.clusters.samplecluster3=aps05
```

4. Save the file with the `PlatformServices.properties` name.

5. Restart the web application server.

The new properties take affect only after the modified `BOE` web application is redeployed on the computer running the web application server. Use `WDeploy` to redeploy the `WAR` file on the web application server. For more information on using `WDeploy`, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

#### 8.1.8.1.4 Changing the name of a CMS cluster

This procedure allows you to change the name of a cluster that is already installed. After changing the name of the CMS cluster, the Server Intelligences Agent automatically reconfigures each SAP Business Objects server so that it registers with the CMS cluster, rather than with an individual CMS.

**Note:**

For experienced administrators of Information platform services, 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.
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 *Information platform services Administrator's Guide*.

## **8.1.9 Managing server groups**

Server groups provide a way of organizing your Information platform services 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 Information platform services 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 improve 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.

### 8.1.9.1 Creating a server group

To create a server group, you need to specify the name and description of the group, and then add servers to the group.

#### 8.1.9.1.1 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. If you want to include additional information about the server group, type it in the **Description** field.
5. Click **OK**.
6. In the "Servers" management area, click **Server Groups** in the navigation tree and select the new server group.
7. Choose **Add Members** from the **Actions** menu.
8. Select the servers that you want to add to this group; then click **>**.

**Tip:**

Use **CTRL + click** to select multiple servers.

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.

#### Related Topics

- [Viewing the state of servers](#)

### 8.1.9.2 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.

#### 8.1.9.2.1 To add subgroups to a server group

1. Go to the "Servers" management area of the CMC.
2. Click **Server Groups** in the navigation tree and select the server group you want to add subgroups to.

This group is the parent group.

3. Choose **Add Members** from the **Actions** menu.
4. Click **Server Groups** in the navigation tree, select the server groups that you want to add to this group, and then click >.

**Tip:**

Use **CTRL + click** to select multiple server groups.

5. Click **OK**.

You are returned to the "Servers" management area, which now lists the server groups that you added to the parent group.

#### 8.1.9.2.2 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 >.

**Tip:**

Use **CTRL + click** to select multiple server groups.

5. Click **OK**.

### 8.1.9.3 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.

#### 8.1.9.3.1 To modify a server's group membership

1. Go to the "Servers" management area of the CMC.
2. Right-click the server whose membership information you want to change, and select **Existing Server Groups**.  
In the details panel, the **Available server groups** list displays the groups you can add the server to. The **Member of Server Groups** list displays any server groups that the server currently belongs to.
3. To change the groups that the server is a member of, use the arrows to move server groups between the lists, then click **OK**.

### 8.1.9.4 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 Information platform services 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 Information platform services server administration tasks to other people. Or you may want different groups within your organization to have control over their own server management.

#### 8.1.9.4.1 To grant access to a server or server group

1. Go to the "Servers" management area of the CMC.
2. Right-click the server or server group you want to grant access to and select **User Security**.
3. 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.
4. Select the user or group you want to grant access to the specified server or server group, then click **>**.
5. Click **Add and Assign Security**.

6. On the "Assign Security" screen, choose the security settings you want for the user or group, and click **OK**.

For detailed information about assigning rights, refer to the Setting Rights chapter.

#### 8.1.9.4.2 Object rights for the Report Application Server

To allow users to create or modify reports over the Web through the Report Application Server (RAS), you must have RAS Report Modification licenses available on your system. You must also grant users a minimum set of object rights. When you grant users these rights to a report object, they can select the report as a data source for a new report or modify the report directly:

- View objects (or "View document instances" as appropriate)
- Edit objects
- Refresh the report's data
- Export the report's data

User must also have permission to add objects to at least one folder before they can save new reports back to Information platform services.

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.

## 8.1.10 Assessing your system's performance

### 8.1.10.1 Monitoring Information platform services servers

The Monitoring application provides the ability to capture the runtime and historical metrics of Information platform services servers, for reporting and notification. The application helps system administrators to identify if servers are functioning normally and if the response times are as expected.

**Related Topics**

- [About Monitoring](#)

## 8.1.10.2 Analyzing server metrics

The Central Management Console (CMC) allows you to view the metrics for the servers in your system. These metrics include general information about each machine, along with details that are specific to the type of server. The CMC also allows you to view system metrics, which include information about your product version, your CMS, and your current system activity.

**Note:**

You can only view the metrics for servers that are currently running.

### 8.1.10.2.1 To view server metrics

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

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

**Related Topics**

- [To change a server's properties](#)
- [About the Server Metrics Appendix](#)

## 8.1.10.3 Viewing system metrics

The "Settings" management area of the CMC displays system metrics that provide general information about your Information platform services 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.

### 8.1.10.3.1 To view system metrics

- In the "Settings" management area of the CMC, click the arrow to expand and view settings for the "Properties", "View global system metrics", "Cluster", and "Hot Backup" sections.

**Related Topics**

- [Managing License keys](#)
- [Clustering Central Management Servers](#)

**8.1.10.4 Logging server activity**

Information platform services allows you to log specific information about Information platform services web activity.

- In addition, each of the Information platform services servers is designed to log messages to your operating system's standard system log.
  - On Windows, Information platform services logs to the Event Log service. You can view the results with the Event Viewer (in the Application Log).
  - On UNIX, Information platform services logs to the syslog daemon as a User application. Each server prepends its name and PID to any messages that it logs.

Each server also logs assert messages to the logging directory of your product installation. The programmatic information logged to these files is typically useful only to SAP 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 `<INSTALLDIR>\Information platform services __MINI-BOE-VERSION__\Logging`.
- On UNIX, the default logging directory `<INSTALLDIR>/sap_bobj/logging` directory of your installation.

The important point to note is that these log files are cleaned up automatically, so there will never be more than approximately 1 MB of logged data per server.

**Note:**

To enable logging to function on UNIX machines that are hosting Information platform services servers, you must set up and configure system logging so that all messages logged to the “user” facility of “info” level or higher are recorded. You must also configure `SYSLOGD` to accept remote logging.

Setup procedures vary from system to system. Consult your operating system documentation for specific instructions.

**8.1.11 Configuring server settings**

This section includes technical information and procedures that show how you can modify settings for Information platform services servers.

The majority of the settings discussed in this section allow you to integrate Information platform services more effectively with your current hardware, software, and network configurations. Consequently, the settings that you choose will depend largely upon your own requirements.

You can change server settings through the Central Management Console (CMC) in two ways.

- On "Properties" screen for the server.
- On the "Edit Common Services" screen for the server.

It is important to note that not all changes occur immediately. If a setting cannot change immediately, the "Properties" and "Edit Common Services" screens display both the current setting (in red text) and the desired setting. When you return to the Servers management area, the server will be marked as Stale. When you restart the server, it will use the desired settings and the Stale flag is removed from the server.

**Note:**

This section does not show how to configure your Web application server to deploy Information platform services applications. This task is typically performed when you install the product. For details, see the *Information platform services Installation Guide*.

**Related Topics**

- [Configuring port numbers](#)
- [To change a server's properties](#)

### **8.1.11.1 To change a server's properties**

1. Go to the "Servers" management area of the CMC.
2. Double-click the server whose settings you want to change.  
The "Properties" screen appears.
3. Make the changes you want, then click **Save** or **Save & Close**.

**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.

### 8.1.11.2 To apply service settings to multiple servers

You can apply the same setting to services that are hosted on multiple servers.

1. Go to the "Servers" management area of the CMC.
2. Pressing **Ctrl**, click each server that hosts services for which you want to change settings, and then right-click and select **Edit Common Services**.

The "Edit Common Services" dialog box appears, displaying a list of services hosted on the servers you selected that have settings you can change.

3. If the "Edit Common Services" dialog box lists more than one service, select the service you want to edit, and click **Continue**.
4. Make changes as needed, and click **OK**.

**Note:**

You are redirected to the "Servers" management area of the CMC. If a server requires a restart, the server is marked as Stale. When you restart the server, it uses the new settings and the Stale flag is removed.

### 8.1.11.3 Working with configuration templates

Configuration templates allow you to easily configure multiple instances of servers. Configuration templates store a list of settings for each service type, which you can use to configure additional server instances. For example, if you have a dozen Web Intelligence Processing Servers that you want to configure identically, you only need to configure settings for one of them. You can then use the configured service to define the configuration template for Web Intelligence Processing Servers, and then apply the template to the other 11 service instances.

Each type of Information platform services service has its own configuration template. For example, there is one configuration template for the Web Intelligence Processing service type, one for the Publishing service type, and so on. The configuration template is defined in the server properties in the Central Management Console (CMC).

When you make a server use a configuration template, existing settings for the server are overwritten with the values from the template. If you later decide to stop using the template, the original settings are not restored. Subsequent changes to the configuration template no longer affect the server.

It is good practice to use configuration templates as follows:

1. Set the configuration template on one server.
2. Assuming you want the same configuration on all servers of the same type, check **Use Configuration Template** for all servers of the same type, including the one where you set the configuration template.

3. Later, if you want to change the configuration of all services of this type, view the properties of any one of the services, deselect the **Use Configuration Template** check box. Change the settings you want, then select **Set Configuration Template** for this server and click **Save**. All services of that type are updated. By not having a server that is always set as the configuration template, you ensure that you will not accidentally change configuration settings for all servers of that type.

#### **Related Topics**

- [To set a configuration template](#)
- [To apply a configuration template to a server](#)

#### **8.1.11.3.1 To set a configuration template**

You can set a configuration template for each type of service. You cannot set multiple configuration templates for a service. You can use any server's "Properties" page to configure the settings that will be used by the configuration template for a service type that is hosted on the server.

1. Go to the "Servers" management area of the CMC.
2. Double-click the server that hosts services whose configuration template you want to set.  
The "Properties" screen appears.
3. Configure the service settings that you want to use in the template, select the **Set Configuration Template** check box and click **Save** or **Save & Close**.

The configuration template for the service type that you selected is defined according to the settings of the current server. Other servers of the same type hosting the same services will be automatically and immediately reconfigured to match the configuration template if they have the **Use Configuration Template** option enabled in their properties.

#### **Note:**

If you don't explicitly define the settings for the configuration template, the service's default settings are used.

#### **Related Topics**

- [To apply a configuration template to a server](#)

#### **8.1.11.3.2 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.

#### **Note:**

Servers that do not have the Use Configuration Template setting enabled will not be updated when you modify the settings of the configuration template.

1. Go to the "Servers" management area of the CMC.
2. Double-click the server that is hosting a service you want to apply the configuration template to.  
The "Properties" screen appears.

3. Select the **Use Configuration Template** check box and click **Save** or **Save & Close**.

**Note:**

If the server requires you to restart it in order for the new settings to take effect, it will show up as "stale" in the servers list.

The appropriate configuration template is applied to the current server. Any subsequent changes to the configuration template change the configuration of all servers that use the configuration template.

Unchecking **Use Configuration Template** does not restore the server configuration to the values as they were when the configuration template was applied. Subsequent changes to the configuration template do not affect the configuration of the servers that are using the configuration template.

**Related Topics**

- [To set a configuration template](#)

#### 8.1.11.3.3 To restore system defaults

You may want to restore a service's configuration to the settings it was initially installed with (for example, if you misconfigure the servers, or experience performance issues).

1. Go to the "Servers" management area of the CMC.
2. Double-click the server hosting a service that you want to restore system defaults for.  
The "Properties" screen appears.
3. Select the **Restore System Defaults** check box and click **Save** or **Save & Close**.  
The default settings for the particular service type are restored.

## 8.1.12 Configuring server network settings

The networking settings for Information platform services 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 Information platform services servers dynamically bind to available ports. Port numbers are automatically managed by Information platform services, but you can use the CMC to specify port numbers.

### 8.1.12.1 Network environment options

Information platform services supports both Internet Protocol 6 (IPv6) and Internet Protocol version 4 (IPv4) network traffic. You can use the server and client components in any of the following environments:

- IPv4 network: all server and client components run with IPv4 protocol only.
- 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. Information platform services does not provide a mechanism to designate a networking environment. You can use the CMC to bind to a specific IPv6 or IPv4 address for any of your Information platform services servers.

#### 8.1.12.1.1 Mixed IPv6/IPv4 environment

The IPv6/IPv4 networking environment enables the following:

- Information platform services 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.

#### 8.1.12.2 Server host identification options

Host identification options can be specified in the CMC for every Information platform services 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 <b>Auto-Assign</b> is selected, the server automatically binds the server's Request Port onto the first network interface on the machine.</p> <p><b>Note:</b> It is good practice to select the Auto-Assign check box 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. See the information about configuring a multihomed machine and working with firewalls in the <i>Information platform services Administrator's Guide</i>.</p>
Hostname	<p>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.</p>
IP Address	<p>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.</p>

**Caution:**

If you specify **Auto assign** on a multi-homed 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 .

**Note:**

If you are working with multi-homed machines or in certain NAT firewall configurations, you may need to specify the Host Name using fully qualified domain names instead of host names.

**Related Topics**

- [To configure the system for firewalls](#)
- [Configuring a multi-homed machine](#)
- [To troubleshoot multiple network interfaces](#)

**8.1.12.2.1 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
<b>Auto assign</b>	The server will bind to one of the available network interfaces.
<b>Hostname</b>	Enter the host name of the network interface on which server listens for requests.
<b>IP Address</b>	Enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface on which server listens for requests.  <b>Note:</b> 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.

### 8.1.12.3 Configuring a multi-homed machine

A multi-homed machine is one that has multiple network addresses. You may accomplish this with multiple network interfaces, each with one or more IP addresses, or with a single network interface that has been assigned multiple IP addresses.

If you have multiple network interfaces, each with a single IP address, change the binding order so that the network interface at the top of the binding order is the one you want the Information platform services 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 Information platform services server. It can be specified by host name or IP address.

**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 Information platform services server components. In this example, the DNS must route communications from the other Information platform services servers to the private address of the File Repository Servers.

**Related Topics**

- [To troubleshoot multiple network interfaces](#)

### 8.1.12.3.1 To configure 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.

1. Go to the **Servers** management area of the CMC.
2. Double-click the CMS.
3. Under "Common Settings", select one of the following options:
  - **Hostname**
  - Enter the host name of the network interface to which the server will bind.
  - **IP Address**
  - Enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface to which the server will bind.

**Note:**

To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

**Caution:**

Do not select Auto assign.

4. For **Request Port** you can do one of the following:
  - Select the **Auto assign** option.
  - Enter a valid port number in the **Request Port** field.
5. Make sure that a port number is specified in the Name Server Port dialog box.

**Note:**

The default port number is 6400.

### 8.1.12.3.2 Configuring the remaining servers to bind to a network address

The remaining Information platform services servers select their ports dynamically by default. For information on disabling the Auto assign setting that dynamically propagates this information, see "To change the port a server uses for accepting requests".

**Related Topics**

- [To change the port a server uses for accepting requests](#)

### 8.1.12.3.3 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 Information platform services to bind to a non-primary routable network interface. Perform

these steps immediately after installing Information platform services on the local machine, before you install Information platform services 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.

### 8.1.12.4 Configuring port numbers

During installation, the CMS is set up to use default port numbers. The default CMS port number is 6400. This port falls within the range of ports reserved by SAP Business Objects (6400 to 6410). Communication on these ports should not conflict with third-party applications.

When started and enabled, each of the other Information platform services servers dynamically binds to an available port (higher than 1024), registers with this port on the CMS, and then listens for Information platform services 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 <b>Auto assign</b> is selected, the server automatically uses an OS-assigned port number.	Specifies the port on which the server listens for all requests. When <b>Auto assign</b> is selected, the server automatically uses a port number assigned by the OS.
Name Server Port	Specifies the Information platform services port on which the CMS listens for name service requests. The default is 6400.	Not applicable.

#### 8.1.12.4.1 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. If no CMS is running on the cluster, you must use the CCM on Windows, or the `serverconfig.sh` script on UNIX, to change the port number.

**Note:**

The CMS uses the same network interface card for the request port and the name server port.

1. Go to the "Servers" management area of the CMC.
2. Double-click the CMS in the server list.
3. Replace the **Name Server Port** number with the port that you want the CMS to listen on. (The default port is 6400.)
4. Click **Save & Close**.

## 5. Restart the CMS.

The CMS begins listening on the port number you specified. The Server Intelligence Agent dynamically propagates the new settings to the other servers on the node, if those servers have the **Auto assign** option selected for the request port. (It may take several minutes for your changes to appear in the Properties settings of all node members.)

The settings you choose on the "Properties" page are reflected in the server command line, which also appears on the "Properties" page.

### 8.1.12.4.2 To change the default CMS port in the CCM on Windows

If no CMS is accessible on the cluster and you want to modify the default CMS port for one or more CMSs in your deployment, you must use the CCM to change the CMS port number.

1. Open the CCM and stop the SIA for the node.
2. Right-click the SIA and choose **Properties**.
3. In the "Properties" dialog box, click the "Startup" tab.
4. From the "Local CMS Servers" list select the CMS that you want to change the port number for, and click **Properties**.
5. To bind the CMS to a specific port, type in the **Port** field one of the following:
  - port number
  - the hostname and port number (use the hostname:port number format)
  - the IP address 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.

### 8.1.12.4.3 To change the default CMS port in the CCM on Unix

If no CMS is accessible on the cluster and you want to modify the default CMS port for one or more CMSs in your deployment, you must use the `serverconfig.sh` script to change the CMS port number.

1. Use the `ccm.sh` script to stop the Server Intelligence Agent (SIA) that hosts the CMS whose port number you want to change.
2. Run the `serverconfig.sh` script. By default this script is in the `<InstallDir>/sap_bobj` directory by default.
3. Select **3 - Modify node**, and press **Enter**.
4. Select the node that hosts the CMS that you want to modify, and press **Enter**.
5. Select **4 - Modify a local CMS** and press **Enter**.

A list of CMSs currently hosted on the node appears.
6. Select the CMS that you want to modify and press **Enter**.
7. Type the new port number for the CMS and press **Enter**.
8. Specify whether you want the CMS to automatically start when the SIA starts, and press **Enter**.
9. Type the command-line arguments for the CMS or accept the current arguments, and press **Enter**.
10. Type quit to exit the script.

11. Start the SIA with the `ccm.sh` script, and wait for the servers to start.

#### 8.1.12.4.4 To change the port a server uses for accepting requests

1. Go to the "Servers" management area of the CMC.
2. Select the server, then choose **Stop Server** from the **Actions** menu.
3. Double-click the server.  
The "Properties" screen appears.
4. Under "Common Settings", deselect the **Auto assign** check box for **Request Port**, then type the port number you want the server to listen on.
5. Click **Save** or **Save & Close**.
6. Start and enable the server.

The server binds to the new port, registers with the CMS, and begins listening for Information platform services requests on the new port.

## 8.1.13 Managing Nodes

### 8.1.13.1 Using nodes

A node is a group of SAP BusinessObjects Business Intelligence platform servers that run on the same host and are managed by the same Server Intelligence Agent (SIA). All servers on a node run under the same user account.

One machine can contain many nodes, so you can run processes under different user accounts.

One SIA manages and monitors all of the servers on a node, ensuring they operate properly.

#### **Note:**

You must use an Administrator account with Enterprise authentication to perform all node management procedures securely. However, if SSL communication between servers is enabled, you must disable SSL to perform any node management procedures (by clearing the **Enable SSL** check box). For more information, see "To configure the SSL protocol in the CCM" in this guide.

#### **Caution:**

BI platform supports SQL Anywhere databases as ODBC data sources. Before performing node management operations with SQL Anywhere on a Unix machine, you must create an `odbc.ini` file and source it.

### 8.1.13.1.1 Variables

Variable	Description
<INSTALLDIR>	The directory where Information platform services is installed. <ul style="list-style-type: none"> <li>On Windows: C:\Program Files (x86)\SAP BusinessObjects</li> </ul>
<SCRIPTDIR>	The directory where node management scripts are located. <ul style="list-style-type: none"> <li>On Windows: &lt;INSTALLDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts</li> <li>On Unix: &lt;INSTALLDIR&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM64&gt;/scripts</li> </ul>
<PLATFORM32>	The name of your Unix operating system. Acceptable values are: <ul style="list-style-type: none"> <li>aix_rs6000</li> <li>linux_x86</li> <li>solaris_sparc</li> <li>win32_x86</li> </ul>
<PLATFORM64>	The name of your Unix operating system. Acceptable values are: <ul style="list-style-type: none"> <li>aix_rs6000_64</li> <li>linux_x64</li> <li>solaris_sparcv9</li> <li>win64_x64</li> </ul>

### 8.1.13.2 Adding a new node

The installation program creates nodes when you first install Information platform services.

You may need additional nodes if you want to add a new machine to an existing cluster to improve the cluster's performance, or if you want to run servers under different user accounts with an existing deployment.

You can add a new node using the Central Configuration Manager (CCM), or using a node management script. If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

**Remember:**

You can add a node only on the machine where the node is located.

#### 8.1.13.2.1 Adding a node to a new machine on an existing deployment

You can automatically create the first node on a machine when you use the installation program to add a new machine to an existing deployment.

**Tip:**

During the installation, click **Expand**, and specify your existing Central Management Server.

If you want to create additional nodes, use the Central Configuration Manager or the script.

For more information on installation, see the *Information platform services Installation Guide*.

#### 8.1.13.2.2 To add a node on Windows

**Caution:**

Back up the server configuration for the entire cluster before and after you add a node.

1. In the Central Configuration Manager (CCM), on the toolbar, click **Add Node**.
2. In the "Add Node Wizard", enter the node name and port number for the new Server Intelligence Agent (SIA).
3. Choose whether you want to create servers on the new node.
  - **Add node with no servers**
  - **Add node with CMS**
  - **Add node with default servers**

This option creates only the servers installed on this machine. It does not include all possible servers.

4. Select a CMS.
  - If your deployment is running, select **Use existing running CMS**, and click **Next**.  
If prompted, enter the host name and port for the existing CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key.
  - If your deployment is stopped, select **Start a new temporary CMS**, and click **Next**.  
If prompted, enter the host name and port for the temporary CMS, the Administrator credentials, the data source name, the database credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

**Caution:**

Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

5. Review the confirmation page, and click **Finish**.

The CCM creates a node. If any errors occur, review the log file.

You can now use the CCM to start the new node.

### Adding a node on Windows using a script

**Caution:**

Back up the server configuration for the entire cluster before and after you add a node.

You can use `AddNode.bat` to add a node on a Windows machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

**Example:**

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in the `-connect` string.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldbasesubsystem
-connect "DSN^=BusinessObjects^ CMS^ 140^;UID^=username^;PWD^=Password1^;HOSTNAME^=database^;PORT^=3306"
-dbkey abc1234
```

**Note:**

To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

---

**Related Topics**

- [Variables](#)
- [Script parameters for adding, recreating, and deleting nodes](#)

#### 8.1.13.2.3 To add a node on Unix

**Caution:**

Back up the server configuration for the entire cluster before and after you add a node.

1. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
2. Select **1 - Add node**, and press **Enter**.
3. Type the name of the new node, and press **Enter**.
4. Type the port number of the new SIA, and press **Enter**.
5. Choose whether you want to create servers on the new node.
  - **no servers**  
Creates a node that does not contain any servers.
  - **cms**  
Creates a CMS on the node, but does not create other servers.
  - **default servers**

Creates only the servers installed on this machine. It does not include all possible servers.

**6. Select a CMS.**

- If your deployment is running, select **existing**, and press **Enter**.

If prompted, enter the host name and port for the existing CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key.

- If your deployment is stopped, select **temporary**, and press **Enter**.

If prompted, enter the host name and port for the temporary CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

**Caution:**

Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

**7. Review the confirmation page, and press **Enter**.**

The CCM creates a node. If any errors occur, review the log file.

You can now run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the new node.

### *Adding a node on Unix using a script*

**Caution:**

Back up the server configuration for the entire cluster before and after you add a node.

You can use `addnode.sh` to add a node on a Unix machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

**Example:**

```
<SCRIPTDIR>/addnode.sh -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
-dbkey abc1234
```

---

### **Related Topics**

- [Variables](#)
- [Script parameters for adding, recreating, and deleting nodes](#)

### 8.1.13.3 Recreating a node

You can recreate a node using the Central Configuration Manager (CCM), or using a node management script, after you restore the server configuration for the entire cluster, or if the machine hosting your deployment fails, becomes damaged, or has a corrupt file system. Use the following guidelines:

- It is not necessary to recreate a node if you reinstall the deployment on a replacement machine with identical installation options and node name. The installation program automatically recreates the node.
- A node should be recreated only on a machine with an existing deployment with identical installation options and patch level.
- You should recreate only nodes that do not exist on any machines in your deployment. Ensure that no other machines host the same node.
- Although the deployment allows nodes to run on different operating systems, you should recreate nodes only on machines that use the same operating system.
- If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

**Remember:**

You can recreate a node only on the machine where the node is located.

#### 8.1.13.3.1 To recreate a node on Windows

1. In the Central Configuration Manager (CCM), on the toolbar, click **Add Node**.
2. In the "Add Node Wizard", enter the node name and port number for the recreated Server Intelligence Agent (SIA).

**Note:**

The names of the original and recreated nodes must be identical.

3. Select **Recreate node**, and click **Next**.
  - If the node exists in the system database of the Central Management Server (CMS), it is recreated on the local host.

**Caution:**

Use this option only if the node does not exist on any hosts in the cluster.

- If the node does not exist in the system database of the CMS, a new node with default servers is added. Default servers include all of the servers installed on the host.
4. Select a CMS.
    - If your CMS is running, select **Use existing running CMS**, and click **Next**.  
If prompted, enter the host name and port for the existing CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key.
    - If your CMS is stopped, select **Start a new temporary CMS**, and click **Next**.

If prompted, enter the host name and port for the temporary CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

**Caution:**

Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

5. Review the confirmation page, and click **Finish**.

The CCM recreates the node, and adds information about the node to the local machine. If any errors occur, review the log file.

You can now use the CCM to start the recreated node.

### *Recreating a node on Windows using a script*

You can use `AddNode.bat` to recreate a node on a Windows machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

**Example:**

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in the `-connect` string.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysql databases subsystem
-connect "DSN^=BusinessObjects^ CMS^ 140^;UID^=username^;PWD^=Password1^;HOSTNAME^=database^;PORT^=3306"
-dbkey abc1234
-adopt
```

**Note:**

To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

### **Related Topics**

- [Variables](#)
- [Script parameters for adding, recreating, and deleting nodes](#)

#### 8.1.13.3.2 To recreate a node on Unix

1. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
2. Select **1 - Add node**, and press **Enter**.
3. Type the name of the new node, and press **Enter**.

**Note:**

The names of the original and recreated nodes must be identical.

4. Type the port number of the new SIA, and press **Enter**.
5. Select **recreate node** and press **Enter**.
  - If the node exists in the system database of the Central Management Server (CMS), it is recreated on the local host.

**Caution:**

Use this option only if the node does not exist on any hosts in the cluster.

- If the node does not exist in the system database of the CMS, a new node with default servers is added. Default servers include all of the servers installed on the host.
6. Select a CMS.
    - If your deployment is running, select **existing**, and press **Enter**.

If prompted, enter the host name and port for the existing CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key.
    - If your deployment is stopped, select **temporary**, and press **Enter**.

If prompted, enter the host name and port for the temporary CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

**Caution:**

Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

7. Review the confirmation page, and press **Enter**.

The CCM recreates the node, and adds information about the node to the local machine. If any errors occur, review the log file.

You can now run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the recreated node.

### *Recreating a node on Unix using a script*

You can use `addnode.sh` to recreate a node on a Unix machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

**Example:**

```
<SCRIPTDIR>/addnode.sh -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
-adopt
```

**Related Topics**

- [Variables](#)
- [Script parameters for moving nodes](#)

### 8.1.13.4 Deleting a node

You can delete a stopped node using a running Central Configuration Manager (CCM), or using a node management script. Use the following guidelines:

- Deleting a node also permanently deletes the servers on the node.
- If your cluster has multiple machines, delete the nodes before you remove a machine from the cluster and uninstall the software from it. If you remove a machine from a cluster before deleting a node, or if the file system on a machine malfunctions, you must recreate the node on a different machine with the same servers, in the same cluster, and then delete the node.

**Remember:**

You can delete a node only on the machine where the node is located.

**Related Topics**

- [Recreating a node](#)

#### 8.1.13.4.1 To delete a node on Windows

**Caution:**

Back up the server configuration for the entire cluster before and after you delete a node.

1. Run the Central Configuration Manager (CCM).
2. In the CCM, stop the node that you want to delete.
3. Select the node, and click **Delete Node** on the toolbar.
4. If prompted, enter the hostname, port, and Administrator credentials for the CMS.

The CCM deletes the node and all the servers on the node.

#### *Deleting a node on Windows using a script*

**Caution:**

Back up the server configuration for the entire cluster before and after you delete a node.

You can use `RemoveNode.bat` to delete a node on a Windows machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

**Example:**

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
-cms mycms:6400
-username Administrator
-password Password1
```

---

**Related Topics**

- [Variables](#)
- [Script parameters for adding, recreating, and deleting nodes](#)

**8.1.13.4.2 To delete a node on Unix****Caution:**

Back up the server configuration for the entire cluster before and after you delete a node.

1. Run `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>` to stop the node that you want to delete.
2. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
3. Select **2 - Delete node**, and press **Enter**.
4. Select the node you want to delete, and press **Enter**.
5. If prompted, enter the hostname, port, and Administrator credentials for the CMS.

The node and all the servers on the node are deleted.

*Deleting a node on Unix using a script***Caution:**

Back up the server configuration for the entire cluster before and after you delete a node.

You can use `removenode.sh` to delete a node on a Unix machine. For more information, see the “Script parameters for adding, recreating, and deleting nodes” section.

**Example:**

```
<SCRIPTDIR>\RemoveNode.sh -name mynode2
-cms mycms:6400
-username Administrator
-password Password1
```

---

**Related Topics**

- [Variables](#)
- [Script parameters for adding, recreating, and deleting nodes](#)

### 8.1.13.5 Renaming a node

You can rename a node using the Central Configuration Manager (CCM). In order to rename a node, you must create a new node with a new name, clone the servers from the original node to the new node, and then delete the original node. Use the following guidelines:

- If you rename the machine where a node is located, you do not need to rename the node. You can continue to use the existing node name.
- If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

**Remember:**

You can rename a node only on the machine where the node is located.

**Related Topics**

- [Adding a new node](#)
- [Cloning servers](#)
- [Deleting a node](#)

#### 8.1.13.5.1 To rename a node on Windows

**Caution:**

Back up the server configuration for the entire cluster before and after you rename a node.

1. Start the Central Configuration Manager (CCM).
2. In the Central Configuration Manager (CCM), on the toolbar, click **Add Node**.
3. In the "Add Node Wizard", enter the node name and port number for the new Server Intelligence Agent (SIA), the Administrator credentials, the database connection information, the credentials for the system database, and the cluster key.
4. Select **Add node with no servers**.
5. After the node is created, use the "Server Management" page of the Central Management Console to clone all of the servers from the original node to the new node.

**Note:**

Ensure that the cloned servers have no port conflicts with servers on the old node.

6. In the CCM, start the new node.
7. After the new node has been running for five minutes, use the CCM to delete the original node.

**Related Topics**

- [Adding a new node](#)
- [Cloning servers](#)
- [Deleting a node](#)

### 8.1.13.5.2 To rename a node on Unix

**Caution:**

Back up the server configuration for the entire cluster before and after you rename a node.

1. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`.
2. Select **1 - Add node**, and press **Enter**.
3. Type the name of the new node, and press **Enter**.
4. Type the port number of the new SIA, and press **Enter**.
5. If prompted, enter the Administrator credentials, the database connection information, the credentials for the system database, and the cluster key.
6. Select **no servers** and press **Enter**.
7. After the node is created, use the "Server Management" page of the Central Management Console to clone all of the servers from the original node to the new node.

**Note:**

Ensure that the cloned servers have no port conflicts with servers on the old node.

8. Run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the new node.
9. After the new node has been running for five minutes, use `serverconfig.sh` to delete the original node.

**Related Topics**

- [Adding a new node](#)
- [Cloning servers](#)
- [Deleting a node](#)

### 8.1.13.6 Moving a node

You can move a stopped node from one cluster to another using the Central Configuration Manager (CCM), or using a node management script. Use the following guidelines:

- Ensure that the destination cluster does not have a node with the same name.
- Ensure that all server types installed on the machine where the source node is located are also installed on the production cluster.
- If you want to add a new machine to a production cluster but do not want the machine to be usable until you finish testing it, install Information platform services on a stand-alone machine, test the machine, then move the node to a production cluster.

**Remember:**

You can move a node only on the machine where the node is located.

### 8.1.13.6.1 To move an existing node on Windows

In this example, the node that you want to move is installed on the source system. The source system computer was initially a standalone installation, but it is to be added to the destination cluster.

**Caution:**

Back up the server configuration for the entire cluster before and after you move a node.

1. Stop the node in the Central Configuration Manager (CCM).
2. Right-click the node and select **Move**.
3. If prompted, select the data source name, and enter the hostname, the port, the database connection information, the Administrator credentials for the destination CMS, and the cluster key.
4. Select a CMS.
  - If your source deployment is running, select **Use existing running CMS**, and click **Next**.  
If prompted, enter the hostname and port for the source system's existing CMS and the Administrator credentials.
  - If your source deployment is stopped, select **Start a new temporary CMS**, and click **Next**.  
If prompted, enter the hostname and port for the source system's temporary CMS, the Administrator credentials, the data source name, the database credentials for the source system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

**Caution:**

Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

5. Review the confirmation page, and click **Finish**.

The CCM creates a new node on the destination cluster with the same name and the same servers as the node on the source cluster. A copy of the node remains on the source cluster. The configuration templates for the servers in the node do not move. If any errors occur, review the log file.

**Caution:**

Do not use the source cluster after moving the node.

6. In the CCM, start the moved node.

#### *Moving a node on Windows using a script*

**Caution:**

Back up the server configuration for the entire cluster before and after you move a node.

You can use `MoveNode.bat` to move a node on a Windows machine. For more information, see the “Script parameters for moving nodes” section.

**Example:**

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in the `-connect` string.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysqldatabasesubsystem
-connect "DSN^=Source^ BOEXI40^;UID^=username^;PWD^=Password1^;HOSTNAME^=database1^;PORT^=3306"
-dbkey abc1234
-destcms destinationMachine:6401
-destusername Administrator
-destpassword Password2
-destdbdriver sybasedatabasesubsystem
-destconnect "DSN^=Destin^ BOEXI40^;UID^=username^;PWD^=Password2^;"
-destdbkey def5678
```

**Note:**

To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

**Related Topics**

- [Variables](#)
- [Script parameters for moving nodes](#)

**8.1.13.6.2 To move an existing node on Unix**

In this example, the node that you want to move is installed on the source system. The computer was initially part of a standalone cluster, but it is to be added to the destination cluster.

**Caution:**

Back up the server configuration for the entire cluster before and after you move a node.

1. Run `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>` to stop the node.
2. Run `<INSTALLDIR>/sap_bobj/serverconfig.sh`
3. Select **4 - Move node**, and press **Enter**.
4. Select the node you want to move, and press **Enter**.
5. When prompted, select the system database connection information, and enter the hostname, the port, the Administrator credentials for the destination CMS, and the cluster key.
6. Select a CMS.
  - If your source deployment is running, select **existing**, and press **Enter**.  
If prompted, enter the hostname and port for the source system's existing CMS and the Administrator credentials.
  - If your source deployment is stopped, select **temporary**, and press **Enter**.  
If prompted, enter the hostname and port for the source system's temporary CMS, the Administrator credentials, the database connection information and the credentials for the source system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

**Caution:**

Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

7. Review the confirmation page, and press **Enter**.

The CCM creates a new node on the destination cluster with the same name and the same servers as the node on the source cluster. A copy of the node remains on the source cluster. The configuration templates for the servers in the node do not move. If any errors occur, review the log file.

**Caution:**

Do not use the source cluster after moving the node.

8. Run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the moved node.

### *Moving a node on Unix using a script*

**Caution:**

Back up the server configuration for the entire cluster before and after you move a node.

You can use `movenode.sh` to move a node on a Unix machine. For more information, see the “Script parameters for moving nodes” section.

**Example:**

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysqldatabasesubsystem
-connect "DSN=Source BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
-dbkey abc1234
-destcms destinationMachine:6401
-destusername Administrator
-destpassword Password2
-destdbdriver sybasedatabasesubsystem
-destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
-destdbkey def5678
```

---

**Related Topics**

- [Variables](#)
- [Script parameters for moving nodes](#)

## **8.1.13.7 Script parameters**

## 8.1.13.7.1 Script parameters for adding, recreating, and deleting nodes

Parameter	Description	Example
-adopt	Recreates the node if it already exists in the CMS.	-adopt
-cms	The name and port number of the Central Management Server (CMS). <b>Caution:</b> Do not use this parameter if you use <code>-usetempcms</code> . <b>Note:</b> You must specify a port number if the CMS is not running on the default 6400 port.	-cms mycms:6409
-cmsport	<ul style="list-style-type: none"> <li>The port of the CMS when starting a temporary CMS. <b>Restriction:</b> You must also use the <code>-usetempcms</code>, <code>-dbdriver</code>, <code>-connect</code>, and <code>-dbkey</code> parameters.</li> <li>The port of the CMS when creating a new CMS. <b>Restriction:</b> You must also use the <code>-dbdriver</code>, <code>-connect</code>, and <code>-dbkey</code> parameters.</li> </ul>	-cmsport 6401
-connect	The connection string of the CMS or the temporary CMS system database. <b>Note:</b> Omit the <code>HOSTNAME</code> and <code>PORT</code> attributes when connecting to DB2, Oracle, SQL Server, or Sybase databases.	-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"

Parameter	Description	Example
-dbdriver	The database driver of the CMS. Accepted values: <ul style="list-style-type: none"> <li>• db2databasesubsystem</li> <li>• maxdbdatabasesubsystem</li> <li>• mysqldatabasesubsystem</li> <li>• oracledatabasesubsystem</li> <li>• sqlanywheredatabasesubsystem</li> <li>• sqlserverdatabasesubsystem</li> <li>• sybasedatabasesubsystem</li> </ul>	-dbdriver mysqldatabasesubsystem
-dbkey	The cluster key.	-dbkey abc1234
-name	The name of a node.	-name mynode2
-noservers	Creates a node without servers. <b>Note:</b> The additional <code>-createcms</code> parameter creates a node with a CMS, but no other servers. Omit these parameters to create a node with all of the default servers.	-noservers
-password	The password of the Administrator account.	-password Password1
-siaport	The port number of the Server Intelligence Agent for the node.	-siaport 6409
-username	The user name of the Administrator account.	-username Administrator
-usetempcms	<b>Caution:</b> Do not use this parameter if you use <code>-cms</code> . Starts and uses the temporary CMS. <b>Note:</b> Use a temporary CMS when your deployment is not running.	-usetempcms

### Related Topics

- [Adding a node on Windows using a script](#)

- [Adding a node on Unix using a script](#)
- [Recreating a node on Windows using a script](#)
- [Recreating a node on Unix using a script](#)
- [Deleting a node on Windows using a script](#)
- [Deleting a node on Unix using a script](#)

### 8.1.13.7.2 Script parameters for moving nodes

Parameter	Description	Example
-cms	<p>The name of the source Central Management Server (CMS).</p> <p><b>Caution:</b> Do not use this parameter if you use <code>-usetempcms</code></p> <p><b>Note:</b> You must specify a port number if the CMS is not running on the default 6400 port.</p>	-cms sourceMachine:6409
-cmsport	<ul style="list-style-type: none"> <li>• The port of the CMS when starting a temporary CMS.</li> </ul> <p><b>Restriction:</b> You must also use the <code>-usetempcms</code>, <code>-dbdriver</code>, <code>-connect</code>, and <code>-dbkey</code> parameters.</p> <ul style="list-style-type: none"> <li>• The port of the CMS when creating a new CMS.</li> </ul> <p><b>Restriction:</b> You must also use the <code>-dbdriver</code>, <code>-connect</code>, and <code>-dbkey</code> parameters.</p>	-cmsport 6401
-connect	<p>The connection string of the source CMS or the temporary CMS system database.</p> <p><b>Note:</b> Omit the <code>HOSTNAME</code> and <code>PORT</code> attributes when connecting to DB2, Oracle, SQL Server, or Sybase databases.</p>	-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOST NAME=database;PORT=3306"

Parameter	Description	Example
-dbdriver	<p>The database driver of the source CMS.</p> <p>Accepted values:</p> <ul style="list-style-type: none"> <li>• db2databasesubsystem</li> <li>• maxdbdatabasesubsystem</li> <li>• mysqldatabasesubsystem</li> <li>• newdbdatabasesubsystem</li> <li>• oracledatabasesubsystem</li> <li>• sqlanywheredatabasesubsystem</li> <li>• sqlserverdatabasesubsystem</li> <li>• sybasedatabasesubsystem</li> </ul> <p><b>Note:</b> sqlserverdatabase is not supported on Unix.</p>	-dbdriver mysqldatabasesubsystem
-dbkey	The source cluster key.	-dbkey abc1234
-destcms	<p>The name of the destination CMS.</p> <p><b>Note:</b> You must specify a port number if the CMS is not running on the default 6400 port.</p>	-destcms destinationMachine:6401
-destconnect	<p>The connection string of the destination CMS system database.</p> <p><b>Note:</b> Omit the <code>HOSTNAME</code> and <code>PORT</code> attributes when connecting to DB2, Oracle, SQL Server, or Sybase databases.</p>	-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password;HOST NAME=database;PORT=3306"

Parameter	Description	Example
-destdbdriver	<p>The database driver of the destination CMS.</p> <p>Accepted values:</p> <ul style="list-style-type: none"> <li>• db2databasesubsystem</li> <li>• maxdbdatabasesubsystem</li> <li>• mysqldatabasesubsystem</li> <li>• newdbdatabasesubsystem</li> <li>• oracledatabasesubsystem</li> <li>• sqlanywheredatabasesubsystem</li> <li>• sqlserverdatabasesubsystem</li> <li>• sybasedatabasesubsystem</li> </ul> <p><b>Note:</b> sqlserverdatabase is not supported on Unix.</p>	-destdbdriver sybasedatabasesubsystem
-destdbkey	The destination cluster key.	-destdbkey def5678
-destpassword	The password of the Administrator account on the destination CMS.	-destpassword Password2
-destusername	The user name of the Administrator account on the destination CMS.	-destusername Administrator
-password	The password of the Administrator account on the source CMS.	-password Password1
-username	The user name of the Administrator account on the source CMS.	-username Administrator
-usetempcms	<p><b>Caution:</b> Do not use this parameter if you use -cms</p> <p>Starts and uses the temporary CMS.</p> <p><b>Note:</b> Use a temporary CMS when your deployment is not running.</p>	-usetempcms

### Related Topics

- [Moving a node on Windows using a script](#)
- [Moving a node on Unix using a script](#)

### 8.1.13.8 Adding Windows server dependencies

In a Windows environment, each instance of the Server Intelligence Agent (SIA) depends on the Event Log and Remote Procedure Call (RPC) services.

If a SIA does not operate correctly, ensure that both services appear on the SIA's "Dependency" tab.

#### 8.1.13.8.1 To add Windows server dependencies

1. Use the Central Configuration Manager (CCM) to stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and select **Properties**.
3. Click the **Dependency** tab.
4. Click **Add**.  
The "Add Dependency" dialog box appears, displaying a list of all available dependencies.
5. Select a dependency, and click **Add**.
6. Click **OK**.
7. Use the CCM to restart the SIA.

### 8.1.13.9 Changing the user credentials for a node

You can use the Central Configuration Manager (CCM) to specify or update the user credentials for the Server Intelligence Agent (SIA) if the operating system password changes, or if you want to run all of the servers on a node under a different user account.

All servers managed by the SIA run under the same account. To run a server using a non-system account, ensure that your account is a member of the Local Administrators group on the server machine, and that it has the "Replace a process level token" right.

#### **Restriction:**

On a Unix machine, you must run Information platform services with the same account that was used to install it. To use a different account, reinstall the deployment using a different account.

#### 8.1.13.9.1 To change the user credentials for a node on Windows

1. Use the Central Configuration Manager (CCM) to stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and select **Properties**.
3. Clear the **System Account** check box.
4. Enter a username and a password, and click **OK**.
5. Use the CCM to restart the SIA.

The SIA and the server processes log onto the local machine with the new user account.

## 8.1.14 Renaming a computer in an Information platform services deployment

You can change the name of a computer in an SAP BusinessObjects Business Intelligence platform deployment at any time by stopping all BI platform servers on the computer and then renaming the computer.

### **Note:**

If this computer is part of a cluster, it is not necessary to stop all computers and servers in the cluster.

If the CMS system database or the auditing database is located on the computer that you are renaming, you must update the database connection information after you rename the computer. If you use ODBC to connect to either of these databases, you must update the connection with the new name of the computer. For all other database connections, you must select the existing database in the Central Configuration Manager (CCM). Update the host file entry for the renamed computer on each computer in the cluster (including computers hosting only Web Tier), so that the computer's old name resolves to the new name.

### **Note:**

If you use SSO, you must update the `cms` value in `jsp-sso-provider.jsp` and the `sso.global.cms` and `sso.trusted.auth.x509.cms` in `sso.properties` to use the correct CMS hostname.

## 8.1.15 Managing server and node placeholders

### 8.1.15.1 To view server placeholders

- In the "Servers" management area of the CMC, right-click a server and select **Placeholders**. The "Placeholders" dialog box displays a list of placeholders for servers on the same cluster as the server you selected. If you want to change the value for a placeholder, modify the placeholder for the node.

#### **Related Topics**

- [Server and node placeholders](#)

### 8.1.15.2 To view and edit the placeholders for a node

**Note:**

You cannot edit the settings for all placeholders. For example, %INSTALLROOTDIR% is auto-populated and is, therefore, read-only.

1. In the "Servers" management area of the Central Management Console, right-click the node for which you want to change the placeholders and select **Placeholders**.
2. If you want to edit any of the settings for the placeholders, make the changes and click **OK** to continue.

**Related Topics**

- [Server and node placeholders](#)

# Managing Web Application Container Servers (WACS)

## 9.1 WACS

### 9.1.1 Web Application Container Server (WACS)

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

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

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

#### Related Topics

- [Common Tasks](#)

#### 9.1.1.1 Do I need WACS?

If you do not want to use a Java application server to host your SAP Business Objects web applications, then you can host them on WACS.

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

### 9.1.1.2 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 SAP.
- WACS removes the need for Java application server administration and maintenance skills.
- WACS provides an administrative interface that is consistent with other Information platform services servers.

### 9.1.1.3 Common Tasks

Task	Description	Topic
How can I improve the performance of web applications or web services that are hosted on WACS.	You can improve the performance of the web applications or web services by installing WACS on multiple machines.	<ul style="list-style-type: none"> <li>• <a href="#">Adding or removing additional WACS to your deployment</a></li> <li>• <a href="#">Cloning a Web Application Container Server</a></li> </ul>
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.	<a href="#">Adding or removing additional WACS to your deployment</a>
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.	<a href="#">Adding or removing additional WACS to your deployment</a>
How can I improve the security of communication between clients and WACS?	Configure HTTPS on WACS.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring HTTPS/SSL</a></li> <li>• <a href="#">Using WACS with firewalls</a></li> </ul>

Task	Description	Topic
How can I improve the security of communication between WACS and other Business Objects servers in my deployment?	Configure SSL communication between WACS and other Information platform services servers in your deployment.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring servers for SSL</a></li> <li>• <a href="#">Using WACS with firewalls</a></li> </ul>
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.	<a href="#">To configure WACS to support HTTPS with a reverse proxy</a>
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"> <li>• <a href="#">Using WACS with other web servers</a></li> <li>• <a href="#">Using WACS with a load balancer</a></li> <li>• <a href="#">Using WACS with a reverse proxy</a></li> <li>• <a href="#">Using WACS with firewalls</a></li> </ul>
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.	<a href="#">Using WACS with a load balancer</a>
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.	<a href="#">Using WACS with a reverse proxy</a>

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"> <li><a href="#">To configure tracing on WACS</a></li> <li><a href="#">To view server metrics</a></li> </ul>
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"> <li>The HTTP, HTTP through proxy, and HTTPS ports that you specified for the WACS have been taken by other applications.</li> <li>The WACS has enough memory allocated to it.</li> <li>The WACS allows enough concurrent requests.</li> <li>If necessary, restore the system defaults for the WACS.</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">To resolve HTTP port conflicts</a></li> <li><a href="#">To change memory settings</a></li> <li><a href="#">To change the number of concurrent requests</a></li> <li><a href="#">To restore system defaults</a></li> </ul>
Where can I find a list of WACS properties?	The "Server Properties Appendix" of this guide contains a list of WACS properties.	<a href="#">Core Services properties</a>

## 9.1.2 Adding or removing additional WACS to your deployment

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

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

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

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

**Note:**

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

### 9.1.2.1 Installing WACS

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

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

- In a Full installation, on the "Select Java Web Application" screen choose **Install Web Application Container Server and automatically deploy web applications and services to it**.

If you select a Java application server in a New installation, WACS is not installed.

- In a Custom / Expand installation, you can choose to install WACS on the "Select Features" screen by expanding **Servers > Platform Services** and selecting **Web Application Container Server**.

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

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

WACS is supported only on Windows operating systems.

**Note:**

The web applications that WACS hosts are automatically deployed when you install WACS or when you apply updates or hot-fixes to WACS or to WACS-hosted web applications. It takes several minutes for the web applications to deploy. The WACS will be in the "Initializing" state until the web application deployment is complete. Users will not be able to access web applications hosted on WACS until the web applications are fully deployed. Do not stop the server until the initial deployment is completed. You can view the server state of the WACS through the Central Configuration Manager (CCM).

This delay occurs only when starting WACS the first time after installing WACS or applying updates to it. This delay does not occur for subsequent WACS restarts.

Web applications cannot be manually deployed to a WACS server. You cannot use WDeploy to deploy web applications to WACS.

### 9.1.2.2 Adding a new Web Application Container Server

Because it uses a lot of resources, run only one Web Application Container Server (WACS) at a time on a computer. To help recover in the event of a misconfigured WACS, you can deploy more than one WACS on the same computer but run one server.

The TraceLog Service (for server tracing) is created automatically when you create a new WACS.

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

**Note:**

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

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

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

### 9.1.2.3 Cloning a Web Application Container Server

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

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

**Note:**

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

1. Go to the "Servers" management area of the CMC.
2. Select the WACS that you want to clone, right-click and select **Clone Server**.  
The "Clone Server" screen displays a list of nodes in your deployment that you can clone the WACS to. Only those nodes that have WACS installed appear in the **Clone to Node** list.
3. On the "Clone Server" screen, type a new server name, select the node that you want to clone the server to, and click **OK**.

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

**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**

- [Resolving port conflicts](#)

### 9.1.2.4 Deleting WACS from your deployment

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

1. Go to the "Servers" management area of the CMC.
2. Stop the server that you want to delete by right-clicking the server and clicking **Stop Server**.
3. Right-click the server and select **Delete**.

4. When prompted for confirmation, click **OK**.

## 9.1.3 Adding or removing services to WACS

### 9.1.3.1 To add a web application or web service to a WACS

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

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

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

If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running BOE Web Application Service on another WACS in your deployment. If you do, click **OK**, log on to another WACS, and start this procedure from the beginning.

5. Right-click the server and choose **Select Services**.  
The "Select Services" screen appears.
6. Select the service that you want to add to the server, add the service to the server by clicking **>**, and click **OK**.
7. Start the WACS by right-clicking the server and clicking **Start Server**.

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

### 9.1.3.2 To remove a web application or web service from a WACS

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

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

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

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

If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running BOE Web Application Service on another WACS in your deployment. If you do, click **OK**, log on to another WACS, and start this procedure from the beginning.

5. Right-click the WACS and choose **Select Services**.  
The "Select Services" screen appears.
6. Select the service that you want to remove, click **<**, and then click **OK**.
7. Start the WACS by right-clicking the server and clicking **Start Server**.

The service is removed from the WACS.

## 9.1.4 Configuring HTTPS/SSL

You can use the Secure Sockets Layer (SSL) protocol and HTTP for network communication between clients and WACS in your Information platform services deployment. SSL/HTTPS encrypts network traffic and provides improved security.

There are two types of SSL:

- SSL used between Information platform services servers, including WACS and other Information platform services servers in your deployment. This is known as CorbaSSL. For more information on using SSL between the Information platform services servers in your deployment, read about communication between Information platform services components in a firewall in this 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. See the information about using WACS with a reverse proxy in this guide.

To configure HTTPS/SSL on a WACS, you must complete these steps:

- 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

- [To configure the system for firewalls](#)
- [Understanding communication between Information platform services components](#)
- [Using WACS with a reverse proxy](#)

## 9.1.4.1 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 box, 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.

### 9.1.4.2 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.

### 9.1.4.3 To configure HTTPS/SSL

Before you configure HTTPS/SSL on your WACS, ensure that you've already created a PKCS12 file or JKS keystore, and that you've copied or moved the file to the machine that is hosting the WACS.

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

PKCS12 certificate stores and JKS keystores have private keys that are password protected, to prevent unauthorized access. You must specify the password for accessing the private keys, so that WACS can access the private keys.

11. It is recommended that you either use a certificate file store or keystore that either contains a single certificate, or where the certificate that you want to use is listed first. However, if you are using a certificate file store or keystore that contains more than one certificate, and that certificate is not the first one in the filestore, in the **Certificate Alias** field, you must specify the alias for the certificate.
12. If you want the WACS to only accept HTTPS requests from certain clients, enable client authentication. Client authentication doesn't authenticate users. It ensures that WACS only serves HTTPS requests to certain clients.
  - a. Check **Enable Client Authentication**.
  - b. In the **Certificate Trust List File Location**, specify the location of the PCKS12 file or JKS keystore that contains the trust list file.

**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.

## 9.1.5 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

## 9.1.6 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 Windows AD users and groups](#)
- [Windows AD security plug-in](#)
- [Setting up a service account for AD authentication with Kerberos](#)
- [Preparing the servers for Windows AD authentication with Kerberos](#)
- [Enabling Kerberos authentication in the Windows AD plug-in for WACS](#)
- [Creating configuration files](#)
- [Configuring WACS for AD Kerberos](#)
- [Configuring AD Kerberos single sign-on](#)

### 9.1.6.1 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.

#### 9.1.6.1.1 Prerequisites

Before you configure the Windows AD security plug-in for Kerberos, you must have completed the following tasks:

- [Setting up a service account for AD authentication with Kerberos](#)
- [To grant the service account rights](#)
- [Preparing the servers for Windows AD authentication with Kerberos](#)
- "Mapping Windows AD accounts"

#### 9.1.6.1.2 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. Select the **Windows Active Directory Authentication is enabled** check box.
4. Under "Authentication Options", select **Use Kerberos authentication**.
5. In the **Service principal name** box, 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 letters. 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 Information platform services servers or the SPN that maps to this account.

**Related Topics**

- [Configuring AD Kerberos single sign-on](#)

### 9.1.6.2 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.

**9.1.6.2.1 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.

**9.1.6.2.2 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.

### 9.1.6.2.3 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 = CHILD1.DOMAIN03.COM
child1.domain03.com = CHILD1.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
}
CHILD1.DOMAIN03.COM = {
admin_server = testvmw2k08
kdc = testvmw2k08
default_domain = child1.domain03.com
}
CHILD2.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
}
```

### 9.1.6.3 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).

#### 9.1.6.3.1 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.

### 9.1.6.4 Troubleshooting Kerberos

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Kerberos configuration

#### 9.1.6.4.1 To enable Kerberos logging

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

**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.

#### 9.1.6.4.2 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\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.

#### 9.1.6.4.3 Mapped AD user unable to log on to Information platform services on WACS

The following two issues may occur, despite the fact that the users have been mapped to Information platform services.

##### *Logon failure due to different AD UPN and SAM names*

A user's Active Directory ID has successfully been mapped to Information platform services. 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.

## 9.1.7 Configuring AD Kerberos single sign-on

If you are configuring AD Kerberos single sign-on for BI launch pad or Web Services SDK and QaaWS, ensure that you have configured both the WACS and the machine that is hosting WACS for AD Kerberos authentication.

**Note:**

If you will use single sign-on in a reverse proxy environment, see the security section of this guide.

**Related Topics**

- [Configuring WACS for AD Kerberos](#)

### 9.1.7.1 Configuring your computer for AD Kerberos single sign-on

To configure AD Kerberos single sign-on for Web Services SDK and QaaWS, you must first configure the computer that is hosting WACS:

- [To configure constrained delegation for Vintela single sign-on](#)
- "To create an SPN for your web application server"
- "To reset the service account password"
- "To create and place a keytab file"
- "Setting up multiple SPNs"
- [To increase the header size limit of your WACS](#)

The following sections describe how to complete each of these steps.

#### 9.1.7.1.1 Setting up multiple SPNs

Using multiple SPNs is not supported.

#### 9.1.7.1.2 To increase the header size limit of your WACS

Active Directory creates a Kerberos token which is used in the authentication process. This token is stored in the HTTP header. Your WACS will have a default HTTP header size which will be sufficient for most user. This header size can be configured.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS for which you want to change the HTTP header size.  
The "Properties" screen appears.

3. Under the "HTTP Configuration", "Configuration of HTTP through Proxy", or "HTTPS Configuration" section, specify a value in the **Maximum HTTP Header Size (in bytes)** field.
4. Click **Save & Close**.
5. Restart the server.

### 9.1.7.2 Configuring WACS for AD Kerberos single sign-on

You can configure a Web Application Container Server to use AD Kerberos single sign-on. AD Kerberos single sign-on is supported. AD NTLM is not supported.

Before you configure WACS, you must configure AD Kerberos single sign-on for the machine that is hosting the WACS.

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

Active Directory single sign-on is ready for use.

### 9.1.7.3 Configuring Kerberos and single sign-on to the database

Single sign-on to the database is supported for deployments that meet all these requirements:

- The deployment of Information platform services is on WACS.
- WACS 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.

**Note:**

These instructions explain how to configure single sign-on to the database. If you want to configure end-to-end single sign-on to the database, you must also perform the configuration steps required for Vintela single sign-on. For details, see [Configuring AD Kerberos single sign-on](#).

#### 9.1.7.3.1 To enable single sign-on to the database

1. Open the `krb5.ini` file that is being used for your deployment of Information platform services. The default location for this file is the WINNT directory on your web application server.
2. Go to the `[libdefaults]` section of the file.
3. Enter this string prior to the start of the `[realms]` section of the file:

```
forwardable = true
```

4. Save and close the file.
5. Restart your WACS.

## 9.1.8 WACS and your IT environment

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

### 9.1.8.1 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.

### 9.1.8.2 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](#)

## 9.1.8.3 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.

### 9.1.8.3.1 To configure WACS to support HTTP with a reverse proxy

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

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

### 9.1.8.3.2 To configure WACS to support HTTPS with a reverse proxy

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

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

## 9.1.8.4 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 Information platform services servers in your deployment, see the "Understanding communication between Information platform services components" section of the *Information platform services Administrator's Guide*.

### Related Topics

- [Understanding communication between Information platform services components](#)

## 9.1.8.5 To configure WACS on a multihomed computer

A multihomed computer 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" page appears.
3. Under "Web Application Container Service", in the "Configuration of HTTP through Proxy" section, clear the **Bind to all IP addresses** check box, and type an IP address for the WACS to bind to.
4. In the "HTTPS Configuration" section, clear the **Bind to all IP addresses** check box, and type an IP address or hostname for the WACS to bind to.
5. Under "Common Settings", clear **Auto assign**, and specify the hostname or IP address of the NIC used for communication between WACS and other Information platform services servers in your deployment.
6. Click **Save & Close**.
7. Restart the WACS.

## 9.1.9 Troubleshooting

### 9.1.9.1 To configure tracing on WACS

To configure tracing for WACS, see [Logging traces from components](#).

### 9.1.9.2 To view server metrics

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

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

#### Related Topics

- [Web Application Container Server metrics](#)

### 9.1.9.3 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 "List of Running WACS Connectors" metric. If an enabled connector does not appear in the list, the connector has not been configured properly.

### 9.1.9.4 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 HTTPS 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.

#### 9.1.9.4.1 To resolve HTTP port conflicts

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

**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.

#### 9.1.9.4.2 To resolve HTTP through proxy or HTTPS port conflicts

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

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

### 9.1.9.5 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 gigabyte of memory to the server.
  - b. Specify a new value for the parameter.
    - To specify a value in megabytes, use "m". For example, "-Xmx640m" allocates 640 megabytes of memory to the WACS.
    - To specify a value in gigabytes, use "g". For example, "-Xmx2g" allocates two gigabytes of memory to the WACS.
  - c. Click **OK**.
6. On the "Manage Servers" screen, start the WACS.

### 9.1.9.6 To change the number of concurrent requests

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

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

### 9.1.9.7 To restore system defaults

If you have 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 enabled only 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.

### 9.1.9.8 To prevent users from connecting to WACS through HTTP

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

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to modify.  
The "Properties" screen appears.
3. Under Web Application Container Service, clear the **Bind to all IP Addresses** check box.
4. In the **Bind to Hostname or IP address** box, type 127.0.0.1, and click **OK**.
5. To start the WACS, right-click the server and choose **Start Server**.

The WACS that is configured this way accepts only connections from the local machine.

### 9.1.10 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 Services properties](#)



# Backing up and Restoring

## 10.1 Hot backups

The hot backup feature allows you to back up your Business Intelligence platform system while continuing to allow users to use the system normally.

### Prerequisites

It is easiest to restore your system to a specific backup time. For example, if your system backups are performed daily at 3:00 AM, you can easily restore the system to the state it was in when the CMS system backup started (3:00 AM on the date of your choice). After a CMS database or auditing database failure, if you have enabled transaction logging on the CMS database or the auditing database, you can restore the system to the state it was in immediately before the failure.

For maximum safety, save transaction logging records at a different location than your primary database backup records. This ensures that, in case of database failure, you can perform roll-forward operations.

### Note:

- Due to a limitation on transaction log size for IBM DB2, transaction-log-related tasks cannot be performed on DB2 servers.
- We recommend writing the transaction log to a file system other than the main database server system, regularly backing up this transaction log, and keeping it with other files in the backup set.

## 10.2 Enabling hot backups

If your business must continue operating while your system is backing up, you must enable and configure hot backups. When activating the hot backup feature, keep the following considerations in mind:

- Ensure that the **Hot Backup Maximum Duration** time is greater than the maximum time you anticipate the backup operation to take—from the time when the CMS backup begins to the time when the FRS backup ends. If the duration is too short, files may be deleted before the backup has a chance to copy them. Balance this concern against system resources because a high value may slightly increase your FRS file store size.
- Crystal Reports 2011 Designer clients, Web Intelligence Rich Clients, and Universe Design Tool clients older than 4.0 FP3, and custom developed thick client applications compiled against SDKs older than 4.0 FP3 might not support file modification during hot backup. If these client applications

are modifying BI content during backups, they may compromise the quality of data modified during the backup. You can prevent client applications from modifying documents to ensure the consistency of backed up data. Update client applications to 4.0 FP3 when possible. If it is not possible, you may want to explore workaround options. For example, you can advise users of client applications to delete existing objects and save new versions rather than modify the objects.

## 10.2.1 To enable hot backups

1. Open the Central Management Console (CMC).
2. Navigate to the **Settings** page.
3. Click **Enable Hot Backup**.
4. Enter the maximum number of minutes you expect the backup to take under **Hot Backup Max Duration**.

Be sure to include the time required to backup both the CMS database and the file system of the BI platform host-machine.

**Note:**

If the actual duration of the backup exceeds the limit entered here it may cause inconsistencies in the backed up data. To avoid this, it is safer to overestimate the time required.

5. To allow older (before 4.0 FP3) Web Intelligence Rich Client, Crystal Reports Designer, or custom SDK thick-client applications to modify documents on the system, select the **Enable Legacy Applications Support (Backup Limitations)** check box.

**Note:**

Allowing older client applications to modify documents during backup operations may result in inconsistencies in documents modified during the backup. For information about backup limitations, see the enabling hot backup section.

6. Click **Update**.  
Hot backup is enabled.

Once hot backup support is enabled, you can perform backups using your database and file system vendor's backup tools. For information about which files to back up and in what order, see "To perform a cold backup".

# Copying your system

## 11.1 Overview of system copying

This chapter describes how to create a duplicate of your BI platform deployment for testing, standby or other purposes.

## 11.2 Terminology

- Source System: The original BI platform deployment.
- Target System: The new deployment you want to create.
- System Copy: To create a duplicate of an existing BI platform deployment.
- Homogenous System Copy: To create a duplicate system where the source and target systems have the same type of operating system and database.
- Heterogeneous System Copy: To create a duplicate system where the source and target systems use different types of operating systems or databases but are based on the same data.
- Database Copy: To create a duplicate of the CMS system or auditing database using database vendor tools.

## 11.3 Use cases

There are a few different reasons why you may want to create a copy of your system. The following table contains a list of the goals you might want to achieve given the resources you might have, and provides a reference to the most appropriate workflow.

Goal	Resources available	Solution
Copying a set of objects (up to 1,000) between deployments	A system where LCM versioning is in use	Use Lifecycle Manager (LCM) to promote objects between systems. See the <i>Lifecycle management console for SAP BusinessObjects Business Intelligence platform User Guide</i> .
Recover a document or other object that was accidentally deleted	A system where LCM versioning is in use	Use LCM to recover an earlier version of the document. See the <i>Lifecycle management console for SAP BusinessObjects Business Intelligence platform User Guide</i> .
Recover a document or other object that was accidentally deleted	<ul style="list-style-type: none"> <li>• Source System (running or stopped) OR Backups of source system databases and files.</li> <li>AND</li> <li>• Detailed system information described in copying procedure</li> </ul>	<p>Use the System Copy Procedure workflow, starting with "Planning to copy your system", and follow the instructions for the rest of the chapter</p> <p><b>Note:</b> You can create your target system on a computer with an existing BI platform deployment of the same release, support package, and patch level, or a "clean" computer with no BI platform installed.</p>
Create a duplicate system for standby or testing with an identical hardware configuration and IP addresses/machine names	<ul style="list-style-type: none"> <li>• Identical hardware where you intend to recreate the source system</li> <li>AND</li> <li>• Backups of the source system or access to the source system to make a backup from.</li> </ul>	Use the system backup and restore workflow detailed in this guide, see the "Conducting an entire system backup" procedure. Recreate the target system from backups of the source system.
Create a duplicate system for standby, testing, or training that does not have to directly mimic the hardware and IP addresses/machine names of the source system	<ul style="list-style-type: none"> <li>• Source System (running or stopped) OR Backups of source system databases and files.</li> <li>AND</li> <li>• Detailed system information described in copying procedure</li> </ul>	

Goal	Resources available	Solution
		<p>Use the System Copy Procedure workflow, starting with "Planning to copy your system", and follow the instructions for the rest of the chapter</p> <p><b>Note:</b> You can create your target system on a computer with an existing BI platform deployment of the same release, support package, and patch level, or a "clean" computer with no BI platform installed.</p>

## 11.4 Planning to copy your system

There are two stages to copying your system:

1. Making the copy of the source system
2. Recreating the copy on the target environment

These steps do not have to be carried out immediately after each other. You can create your copy and wait some time before proceeding to recreate the copy on the target system. This will mean that the copy will be of the system as it was at the time the copy was created. For example, if you wait one month, the copy will recreate the system as it was one month ago.

After reviewing the use cases in the preceding section and deciding which one best suits your needs, you should develop a system copy plan.

### Create a system copy plan

When planning to copy a system, you should decide on the following details in advance:

- If the source system will be stopped or active while the copy is being made (the procedure can be done under either circumstance)
  - If the source system is stopped, how much downtime will be required
  - Plan time for testing to ensure the integrity of the target system
- Which database tools you want to use for database backup and restoration
- Which machines the target system will be deployed on, and where each node will be hosted
- Which optional components you want to copy
- The database type to use for the target CMS database, and any other optional databases you will be copying

You should also give consideration to the following topics:

- Which BI platform components your source system has installed. You can use the **Add/Remove > Modify** function of the installation program to view the list of currently installed components.
- You may need to tune the target system for better performance if it is installed on different hardware than the source system. See the information about improving your system performance in the *SAP BusinessObjects Business Intelligence sizing companion guide*.
- If you want the target system to report from reporting databases other than the source system databases, you may want to change the database connection information for the reporting databases. You can do this by keeping the same DSN name but pointing to DSN on the target system to another database.

#### Required source system files

- CMS system database
- FRS file store
- Semantic layer configuration files
- Auditing database (optional)
- Monitoring database (optional)
- Lifecycle management subversion database (optional)

## 11.5 Considerations and limitations

You should be aware of the following considerations when making a copy of your BI platform deployment.

Area	Consideration
SAP Business Warehouse integrations	If you are using BI platform and SAP ERP or BW in an integrated environment, before copying your system, read the SAP system copy documentation. The system copy guides are available at <a href="http://www.sdn.sap.com/irj/sdn/systemcopy">http://www.sdn.sap.com/irj/sdn/systemcopy</a> (SMP login required). Choose your SAP NetWeaver version, the relevant copy guides are stored in the installation guides folder.
Program version	The source and target systems must be at the same version, support package, and patch level.
Content and configuration settings	Only the entire source system can be copied. You cannot selectively copy content or system configuration settings.
Installation path	The installation path on the source and target locations must be identical: for example if you installed the source system to C:\BusinessObjects, you must install the target to C:\BusinessObjects.
Host operating system	Source and target operating systems must be the same.

Area	Consideration
CMS database software type	CMS source and target databases must be of the same type. You will have the option of changing to another supported database type after copying the system.
Auditing database software type	<p>If you are copying auditing data, the auditing source and target databases must be of the same type. After the copy has been created, you can establish a new database of a different type.</p> <p><b>Note:</b> If you establish a new database, existing events will not be copied to that database, only new events will be recorded to the new database.</p>
Web tier customization	The copy procedure will not copy web tier components from the source system. If you customized the web tier (modified <code>.properties</code> files in the <code>custom</code> folder, for example) you must manually apply those customizations to the target.
Topics not covered by these instructions	This workflow does not describe how to export or import a database. Use your database vendor tools for database copying and restoring.

The following data will be copied during the system copy procedure:

- The CMS repository database. (contains reports, analytics, folders, rights, users and user groups, server settings, and other BI content and system content)
- The Auditing database. (contains auditing events triggered by BI platform servers or client applications)
- The Monitoring database. (contains trending data from metrics, probes, and watches)
- The Lifecycle Management database. (contains different versions of reports, analytics, other BI resources, and version information)

**Note:**

For a description of the databases and their contents, see the "Databases" section of this guide.

- Semantic layer configuration files

Web tier configuration, search index, and any data not specifically mentioned above are not copied.

### Considerations for file recovery copies

If you are copying a system for the specific purpose of recovering a file that was accidentally deleted, you should be aware of the following additional considerations.

Using your backup, perform the steps in the procedure "To create a system copy on the target system" on the production system.

- Do not install all nodes, just install the first node which will contain the CMS and its database.
- Do not install auditing, LCM, or monitoring databases.
- Do not recreate connections to the auditing or reporting databases.

Use LCM to promote the object you want to recover from the target system to the source system.

## 11.6 System copy procedure

The following procedures guide you through the two stages of copying your BI platform deployment.

### 11.6.1 To perform a system copy export from a source system

You will need to make note of the following information from the source system. If you want to write this information down there is a worksheet you can use at "System copy worksheet".

Property	Location
The CMS cluster key (make sure to keep the record secure).	Created by the system administrator when the BI platform was installed.
The name of the nodes.	Go to the <b>Servers</b> tab of the CMC, on the left tree expand <b>Nodes</b> .
The machine name and the BI platform installation folder for each machine in the deployment.	Go to the <b>Servers</b> tab of the CMC, right-click on the CMS and select <b>Placeholders</b> . Look for the value of the <code>%INSTALLROOTDIR%</code> placeholder.
The BI platform administrator password (make sure to keep the record secure).	Created by the system administrator when the BI platform was installed.
<p>All database connections that might be used by the CMS, and the user names and passwords associated with those connections. This can include auditing database if you want to copy this information. Make sure to get this information for all machines in the cluster.</p> <p><b>Note:</b> If you are copying the auditing database, you also need the auditing database connection names and credentials.</p>	<p>Go to the <b>Servers</b> tab of the CMC, right-click on the CMS and select <b>Metrics</b>.</p> <p>Look for the following metrics:</p> <ul style="list-style-type: none"> <li>• "System Database Connection Name"</li> <li>• "System Database Server Name"</li> <li>• "System Database User Name"</li> <li>• "Data Source Name"</li> <li>• "Auditing Database Connection Name" (optional)</li> <li>• "Auditing Database User Name" (optional)</li> </ul>

Property	Location
<p>For every machine in the cluster, the details (client types, versions) of any other database connections (used by universes and reports for example). Make sure to include user names and passwords.</p>	<p>For Crystal reports that report directly from databases, look at the connection information using the SAP Crystal Reports 2011 or SAP Crystal Reports for Enterprise designers. For universe connection information, use the Information Design Tool (.unx) or Universe design tool (.unv).</p>
<p>The version, support package, and patch level of the source system.</p>	<p>On Windows this can be determined by looking at the "Remove or Change" programs tool.</p> <p>On Unix, you can use the <code>AddOrRemoveProducts.sh</code> utility in the BI platform install directory.</p>
<p>The file store locations for every Input FRS and Output FRS in the deployment.</p>	<p>Go to the <b>Servers</b> tab of the CMC, right-click on the Input or Output FRS and select <b>Properties</b>. Look for the "File Store Directory" property.</p> <p><b>Note:</b> If the value begins with % then this is a placeholder, and you will need to click on <b>Placeholders</b> and make a note of the directory listed under that placeholder.</p>

Property	Location
If you plan to copy Lifecycle management (LCM), the location of the LCM overrides folder and LCM subversion files.	<p>The default folder for Override in Windows installations is <code>&lt;INSTALDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride</code>.</p> <p>The default location for the LCM subversion files in Windows installations is <code>&lt;INSTALDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\CheckOut</code></p>
If you plan on copying the monitoring database, the monitoring database folder.	<p>This is set in the CMC. Go to the <b>Applications</b> management area of the CMC, Select <b>Monitoring Application &gt; Properties</b> and look for the "Trending database backup directory".</p> <p>The default folder in Windows installations is <code>&lt;INSTALDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB</code> by default.</p>
The semantic layer folder path.	<p>The default folder path in Windows installations is <code>&lt;install_dir&gt;\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\</code> by default.</p>

After you've recorded the information above:

1. Use your database vendor backup tools to create a backup copy of the following databases:
  - The CMS system database
  - The auditing database (optional)
2. Using file backup tools, backup the following sets of files:
  - The FRS input and output file stores
  - The monitoring trending database (optional)
  - Lifecycle management subversion database (optional)
  - Configuration files from the semantic layer folder: the `cs.cfg` file in the `connectionServer` folder, and any `.sbo` and `.prm` files in any of its subfolders.

**Note:**

For constraints and a detailed description of this workflow, please see the "Hot backups" section.

Keep the information recorded above with the copy of the databases and files. You may want to keep a second copy which you can update as required for future system copy procedures.

## 11.6.2 To perform a system copy import to a target system

This procedure assumes you have created backup copies of the source deployment databases and system files you want to use in your target system. All backup files must be from the same backup set. You will also need the details (cluster key and database credentials for example) noted in “To perform a system copy export from a source system”.

If the target system will reside in a network location with access to the source system resources, you should ensure the target system does not attempt to access those resources until it has been reconfigured. This can be accomplished by placing a firewall between the target system and the source system resources, or leaving the source system stopped while you start the target system. After the first time you start the target system, the firewall can be removed or the source system can be started.

If the target system already has BI platform installed, ensure it is at the same version, support package, and patch level as the source system at the time the copy was created. Also ensure it uses the same installation path as the source system.

1. On the target system, create the connections to the database or databases where you intend to put the CMS repository, auditing database, and reporting database.

**Note:**

While the connections can point to a different database, they must have the same connection name or DSN and use the same credentials as the source system.

2. Use your database tools to restore the CMS system database and the auditing database (if required) from the source-system backup to the target database.

If the universes or reports on the target system need to use a different reporting database, modify the database connection to point to that database.

If you require further instructions on this step, see the "Restoring your system" topic.

3. If BI platform is installed on the target host system, skip to Step 4. If BI platform is not installed, install the BI platform on the target host system keeping the following steps in mind:
  - a. Install the same program version, support package, and patch level as the source system.
  - b. Use the same installation path as the source system.
  - c. Select the same components that were installed on the source system.
  - d. When the installation program asks you to create the CMS database (and auditing database if applicable), choose the **Use an existing database server** option and enter the connection name and credentials set up in step 1.

**Note:**

Do not choose to reinitialize the CMS database.

- e. When prompted for the **Node Name**, use the same names, port numbers, platform administrator password and cluster key as the source system.

For complete installation instructions, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. When the system has finished installing, go to step 6.

**Note:**

If you are not copying your auditing data from the source system, you can create a new auditing database by configuring auditing during the installation procedure.

4. If the BI platform is already installed, on the target system CMS host computer start the CCM.
5. If the BI platform is already installed, add a new node, using the **Recreate Node** option.
  - a. Use the **Node Name** and **SIA Port Number** from the source system.
  - b. Choose to **Start a new temporary CMS**.
  - c. Select a new **CMS Port Number** (can be any free port) and **CMS Database Type** (matching the restored database type).
  - d. Enter details for the connection the CMS database was restored to in Step 1.
  - e. Enter the cluster key from the source-system.
  - f. Enter the Administrator password from the source system.
6. Restore the Input and Output FRS file stores to the target system file store.
7. Restore the monitoring database folder (if you want to copy monitoring information).
8. Restore the LCM subversion files (if you want to copy LCM information).
9. Restore the semantic layer/connection configuration server files.
10. Restart the target system host computers.
11. If you installed the BI platform on the target system in step 3, apply any support packages or patches required to match the source system.
12. If the target system will run on multiple host computers, repeat steps 1–11 for each host computer. Use the Expand install option when installing additional BI platform nodes, and keep in mind that the same node names as the source system should be used for the additional nodes in the target system.
13. If the target system CMS database will use a different database type from the source system, use the CCM to perform "Copying data from one CMS system database to another", specifying as destination the database you want to use for the copy.

After the system copy of BI platform is performed:

1. The installation of the first node on the target creates a temporary CMS, which will be stopped at the end of the installation. Using the CMC, go to the Servers page and delete this CMS.
2. Run the Repository Diagnostic Tool on the target CMS database.
3. Perform a sanity check on the target system to ensure its integrity.
4. Perform a full search re-index.

# Lifecycle Management

## 12.1 About promotion management

The promotion management application 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.

You can promote a BI resource from one system to another system only if the same version of the SAP BusinessObjects Business Intelligence Platform is installed on both the source and destination systems.

SAP BusinessObjects provides the following tools for importing objects across two SAP BusinessObjects Business Intelligence Platform deployments that are at the same version number:

- The promotion management application

For more information on using the promotion management application, see *Business Intelligence Platform CMC Help*.

- BIAR Command-Line Tool

For more information on using BIAR Command Line Tool, see *Business Intelligence Platform CMC Help*.

## 12.2 Version Management System settings for Lifecycle Management Console

- When Subversion is installed with Business Intelligence platform, settings are automatically configured.
- If you want to configure Subversion, which is installed with the promotion management application, enter values on the "VMS Settings" page in the Administration Options in the Lifecycle Management Console tool. The following figure shows the appropriate values to specify on the "VMS Settings" page:

**Version Management Systems** SubVersion ▼

**SubVersionSettings**

Use as Default VMS

Server Name: development1

Server Port: 3690

User name: lcm

Password: ●●●

Install Path: C:\Program Files (x86)\CollabNet S...

Repository Name: svn\_repository

Workspace Directory: c:\checkout\

- When Subversion is installed after Business Intelligence platform:
  1. Ensure that the Subversion service is running and a repository is created.
  2. Enter values on the "VMS Settings" page in the Administration Options in the Lifecycle Management Console tool.
  3. Restart the SIA.

### Configuring Subversion with Apache HTTP server

1. Install Apache 2.2.4 (or higher).

**Note:**

Specify a port number that is different from 80 (for example, 95). To connect to the Apache server and access the default page, in a browser, type `http://localhost:<port number>/`

2. Install subversion version 1.4.5 or higher (any version that supports http protocol).
3. Stop the Apache server.
4. Open the `httpd.conf` file from `C:\Program Files\Apache Software Foundation\Apache2.2\conf`.
5. Check if the below lines are present in the `httpd.conf` file. If not, add them.

```
LoadModule dav_svn_module C:/Program Files/Subversion/bin/mod_dav_svn.so
```

```
LoadModule authz_svn_module C:/Program Files/Subversion/bin/mod_authz_svn.so
```

```
LoadModule dav_svn_module C:/Program Files/Subversion/bin/mod_dav_svn.so
```

```
LoadModule authz_svn_module C:/Program Files/Subversion/bin/mod_authz_svn.so
```

6. Start the Apache server.

7. Subversion stores content in its repositories. You require at least one repository to store all your data, or multiple repositories, one for each project. The following substeps describes how to configure subversion assuming that multiple repositories are used for two projects, project1 and project2:

- a. Create a directory for all the projects, and then a subdirectory for each of the projects (for example, C:\Repositories\project1, C:\Repositories\project2).

**Note:**

These are the directories that hold the repositories.

- b. Create the repositories using the svnadmin utility as follows:

```
svnadmin create C:\Repositories\project1
```

```
svnadmin create C:\Repositories\project2
```

- c. Open the C:\Program Files\Apache Software Foundation\Apache2.2\conf file, and add the following Access lines in the <Directory> tag to protect your system:

```
<Directory />
  Options FollowSymLinks
  AllowOverride None
  Order Allow,Deny
  Allow from < IP address>
</Directory>
```

- d. At the end of the conf file, type Include c:/etc/subversion.conf to include a Subversion configuration file. This subversion configuration file will be created later.

- e. Create a folder called etc on your C: drive.

- f. Use the following commands to create a user and password file for Apache authentication:

```
cd C:\Program Files\Apache Software Foundation\Apache2.2\bin
```

```
htpasswd -cm C:\etc\svn-auth-file <user name1>
```

```
C:\Program Files\Apache Software
Foundation\Apache2.2\bin>htpasswd -cm C:\etc\svn-auth-file <user
name1>
```

```
New password: <password>
```

```
Re-type new password: <password>
```

**Adding password for user <user name1>**

```
C:\Program Files\Apache Software
Foundation\Apache2.2\bin>htpasswd -m C:\etc\svn-auth-file <user name2>
```

```
New password: <password>
```

```
Re-type new password: <password>
```

**Adding password for user <user name2>**

```
C:\Program Files\Apache Software
Foundation\Apache2.2\bin>htpasswd -m C:\etc\svn-auth-file <user name3>
```

```
New password: <password>
```

```
Re-type new password: <password>
```

**Adding password for user <user name3>**

```
C:\Program Files\Apache Software
Foundation\Apache2.2\bin>htpasswd -m C:\etc\svn-auth-file <user name
4>
```

```
New password: <password>
```

```
Re-type new password: <password>
```

**Adding password for user <user name 4>**

Now you have successfully authenticated the users.

- g.** To configure access rights to the repositories, create a file in the `etc` directory (`C:\etc\svn-acl`) and update the following content in the file:

```
#

# specify groups here
#
[groups]

team1 = <user name 3>, <user name 4>

#
# team1 group has a read/write access to project1 repository

# all subdirectories

# all others have read access only

#
[project1:/]
```

```
@team1 = rw

* = r

#
# project2 repository, only <user name 1> and <user
name 2> have read-write access to project2
#
[project2:/]

<user name 1> = rw
<user name 2> = rw

* = r

#
# user is helping with the time zone part of the project2
#
[project2:/timezone]

<user name 1> = rw

<user name 2> = rw
<user name 3> = rw

* = r
```

#### h. Link the Apache server with Subversion:

- a. In the `C:/etc` folder, create the file `subversion.conf` and add the below content to the file:

```
<Location /project1>

    DAV svn

    SVNPath C:/Repositories/project1

    AuthType Basic
```

```
AuthName "Subversion Project1 repository"
AuthUserFile c:/etc/svn-auth-file
Require valid-user
AuthzSVNAccessFile c:/etc/svn-acl

</Location>
<Location /project2>
  DAV svn
  SVNPath C:/Repositories/project2

  AuthType Basic
  AuthName "Subversion Project2 repository"

  AuthUserFile c:/etc/svn-auth-file
  Require valid-user

  AuthzSVNAccessFile c:/etc/svn-acl
</Location>
```

You can now access the C:\Repositories\project1 repository at <http://subversion/project1> (<http://localhost/project1/>). The access is available to a valid user and a basic HTTP authentication is used.

- i. Perform the following configuration steps in the VMS:

**Remember:**

Before performing the following steps, update the subversion settings for Apache from the "Settings" page in the CMC.

- a. Log on to **CMC > Applications > VMS** and update the following information:

**Server name:** localhost

**Server port:** <Apache port number>

**User name:** <user name>

**Password:** <password>

**Install Path:** <subversion 1.4.5 install location>

**Repository name:** <project name>

**Workspace directory:** c:/httpCheckout

- b. Restart the SIA server.

## 12.2.1 Version Management System Supported Options

The version management application supports the following options:

- The version management feature on a single box setup requires that the default Server Intelligence Agent (SIA) has either System or Domain account.

In a single box setup, all installable components are available on the same system. For example, BusinessObjects Enterprise, promotion management, and version management server are installed on the same system.

- The version management feature on a multi-box setup requires an SIA logged in the Domain account. If the SIA is not logged in the Domain account, you must create a new SIA with a Domain account.

In a multi-box setup, BusinessObjects Enterprise, promotion management, and Version management system clients are installed on one system, and version management servers are installed on another system.

### **Note:**

Before you configure SubVersion and the ClearCase version management systems, you must ensure that the version management system is pre-installed.

## 12.2.2 Configuring ClearCase on BI Platform

You can configure ClearCase on the BI Platform by completing the following steps:

1. Install the Clearcase client on the machine where the BI Platform is installed. For more information on clear case installation and configuration see URL [http://publib.boulder.ibm.com/infocenter/cchelp/v7r0m0/index.jsp?topic=/com.ibm.rational.clearcase.books.cc\\_ms\\_platforms\\_guide.doc/clearcase\\_on\\_windows.htm](http://publib.boulder.ibm.com/infocenter/cchelp/v7r0m0/index.jsp?topic=/com.ibm.rational.clearcase.books.cc_ms_platforms_guide.doc/clearcase_on_windows.htm)
2. Complete the following steps in the Central Configuration Manager:
  - a. Right-click **Server Intelligent Agent** and select **Stop Server**
  - b. Right-Click **Server Intelligent Agent** and select **Properties**.
  - c. Un-check the **System Account** check-box.

- d. In the **User** and **Password** fields enter the Domain Username and Password used earlier in Clear case installation.
  - e. Select **OK** and re-start the machine.
  - f. Log on to the machine using the domain username and password.
3. Create VOB and VIEW in ClearCase using the instruction in <http://www.ibm.com/developerworks/rational/library/1111.html>.
  4. Access the Central Management Console and perform the following steps:
    - a. Choose **Version Management**.
    - b. In VMS Settings, choose **ClearCase**.
    - c. Enter the appropriate values in **VOB Tag Name**, **ClearCase Map drive** and **View Storage Directory** fields.
    - d. Log on to the Version Management System. For additional information on ClearCase, see [http://publib.boulder.ibm.com/infocenter/cchelp/v7r0m0/index.jsp?topic=/com.ibm.rational.clearcase.tutorial.doc/a\\_cr\\_vob\\_cclt.htm](http://publib.boulder.ibm.com/infocenter/cchelp/v7r0m0/index.jsp?topic=/com.ibm.rational.clearcase.tutorial.doc/a_cr_vob_cclt.htm)

ClearCase is configured on the BI Platform.

### 12.2.3 Creating and Configuring SubVersion Repository Manually

This chapter describes how to create a new SubVersion repository for promotion management on an existing SubVersion installation.

SubVersion is an open source version control system from CollabNet Inc, and is released under the Apache License. This tool enables you to maintain versions of source codes, web pages, and documentation. This tool is available as free software.

You can download SubVersion from "<http://www.open.collab.net/downloads/subversion/>"

1. To create the SubVersion (svn) repository, navigate to the folder that has *svnadmin.exe*. For example: `C:\Program Files\Subversion\bin` and enter the following command: `C:\svnadmin create c:\<repository_path>\<repository_name>`  
A configuration subdirectory is created under the SubVersion root directory.
2. Create SVN\_USER and SVN\_PASSWORD.  
To create SVN\_USER and SVN\_PASSWORD, complete the following steps:
  - a. Navigate to `<repository_path>/<repository_name>/`, and open the `conf` folder.
  - b. In the `conf` folder, select the `svnserv.conf` file.
  - c. To enter the database credentials, add the following line:  
`password-db = passwd`
  - d. Return to the `conf` folder, and select the `passwd` file.
  - e. Enter the user name and password in the following format:  
`username=password`. For example, `lcm=123`.
  - f. Save the changes.

The SubVersion user name and password are created. To apply these changes, stop and restart SubVersion. Log into the system by using the new credentials.

### 3. Create the LCM service.

To create the LCM service, complete the following steps:

a. Navigate to the SubVersion install directory that has `svnserve.exe`. For example, `C:\Program Files\SubVersion\bin`.

b. Enter the following command:

```
sc create svn binpath= "c:\Program Files\Subversion\bin\svnserve.exe -
-service -r c:\svn_repository" displayname= "BOE LCM subversion" depend=
tcpip start= auto
```

The "BOE LCM SubVersion" SVN service is created in the Windows services.

c. Select **Start > Programs > Administrative Tools > Services**, and start the "BOE LCM SubVersion" service.

The SubVersion repository is created and configured.

#### Note:

- We recommend that you configure port 3690 for SubVersion.
- For information on configuring SubVersion, see the *BusinessObjects LifeCycle Manager User's Guide*.
- In the promotion management application, in the VMS settings options, you must specify a location in the workspace directory field. When you login to VMS, the workspace directory is automatically created in the specified location.

To change the port number, enter the following command:

```
sc create svn binpath= "C:\Program Files\Subversion\bin\svnserve.exe --listen-
port 3694 --service --root c:\svn_repository" displayname= "BOE LCM Subver
sion" depend= tcpip start= auto
```

## 12.3 BIAR Engine Command-Line Tool

The BIAR Engine Command-Line Tool helps administrators and delegated administrators promote content between Development, Quality Assurance, and Production SAP BusinessObjects Enterprise environments. The tool uses scripting to automate the import and export of objects.

The BIAR Engine Command-Line Tool supports migrating objects only from one SAP BusinessObjects Enterprise XI 4.0 system to another. You cannot use the tool to import objects from BusinessObjects, Crystal Enterprise, or an earlier version of SAP BusinessObjects Enterprise. You must use the SAP BusinessObjects Enterprise Upgrade management tool to import content from previous versions.

The BIAR Engine Command-Line Tool is called `biarengine.jar`. On a Windows environment, this file is located at `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. On Unix, the file is located at `<InstallDir>/sap_bobj/java/lib/`.

**Note:**

- You must have a Java Runtime Environment installed. For supported a list of supported JREs, see the SAP BusinessObjects Enterprise supported platform document guide online on our support web site.
- To use the BIAR Engine Command-Line Tool, you must have the Administrator account credentials for the environment that you are importing content to or from. You can also use a delegated administrator account.
- Using the BIAR Engine Command-Line Tool to import BIAR files generated by SAP BusinessObjects Enterprise Upgrade management tool is not supported.

The BIAR Engine Command-Line Tool imports the following types of objects:

Analysis Connections	Web Intelligence Documents
Analysis Workspaces	LDAP Users
Agnostic Documents	List Of Values (LOVs)
Analytic Objects	Modules
BI Modeler Objects	Object Packages
BI workspaces	Overloads
Business Views	PDFs
Calendars	PowerPoint Presentations
Categories	Profiles
Client Actions	Program Objects
Custom Roles	Prompt Groups
Dashboards Documents	Publications
Discussions	Query as a Web Service
Encyclopedias	Reports
Enterprise User Groups	Report Instances
Enterprise Users	Rich Text Format Documents
Events	Server Groups
Excel Spreadsheets	Shortcuts
Flash Files	Text Files
Folders	Universes
FullClientAddins	WinAD Users
FullClientTemplates	Word Documents
Hyperlinks	XcelsiusDMTemplates

**Importing relationships**

The BIAR Engine Command-Line Tool keeps the relationships between imported objects intact only if both objects are imported together, or if one of the objects already exists on the destination system. 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 system.

### Importing users and groups

If you are importing groups and users into an SAP BusinessObjects Enterprise system, and a group already exists on the destination system, 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 system has additional users that are not contained in the group in the BIAR file, they will not be part of the group after the import occurs.

### Importing rights

The BIAR Engine Command-Line Tool imports rights on an object only if the user or group is either exported with the object or already exists on the destination.

If the object and user or group already exist on the destination system, then the imported rights for that object and user will overwrite the existing rights on the destination system.

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 not 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.

## 12.3.1 Using a 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 SAP BusinessObjects Business Intelligence Platform system to connect to, and so on.

The file must have a `.properties` file extension. For example: `Myproperties.properties`

The properties file can include the following parameters.

Parameter	Allowed Values	Description	Example
<i>Action</i>	exportXML, importXML	Specifies whether the tool imports content from a BIAR file to an SAP BusinessObjects Business Intelligence Platform system, or exports the content from a deployment to a BIAR file.  Mandatory.	Action=exportXML
<i>exportBiarLocation</i>	Free-form text. Must include the .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 the .biar extension.	Specifies where the BIAR file that is to be imported 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 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
<i>exportDependencies</i>	True, False	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 dramatically. Optional. If you don't specify a value, the default is False. Only used if action=exportXML.	exportDependencies=false

Parameter	Allowed Values	Description	Example
<i>includeSecurity</i>	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><b>Note:</b> 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>	includeSecurity=false
<i>exportQuery</i>	Free-form text. This must use the CMS query language format.	<p>Specifies the queries that 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 "exportQuery1", "exportQuery2", and so on.</p> <p>Mandatory if action=exportXML.</p>	exportQuery=select * from ci_Infoobjects where si_name = 'Xtreme Employees' and si_kind = 'Webi'

Parameter	Allowed Values	Description	Example
<code>exportQueriesTotal</code>	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>	<code>exportQueriesTotal=5</code>

**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=mycms:6400
authentication=secEnterprise
```

This is an example of a properties file that exports a Web Intelligence 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=mycms:6400
authentication=secEnterprise
exportDependencies=false
exportQuery= select * from ci_Infoobjects where si_name = 'Xtreme Employees' and si_kind = 'Webi'
```

## 12.3.2 To use the BIAR Engine Command-Line Tool

1. Open a command-line window and navigate to the directory where `biarengine.jar` is located.  
For example, `<InstallDir>\SAP BusinessObjects Enterprise XI4.0\java\lib`.

2. Execute `biarengine.jar`.

For example, `java -jar biarengine.jar <properties file>`

The BIAR Engine Command-Line Tool either exports content from SAP BusinessObjects Business Intelligence Platform deployment to a BIAR file, or imports the content from a BIAR file to a SAP BusinessObjects Business Intelligence Platform deployment, depending on the action parameter in the properties file.



# Monitoring

## 13.1 About Monitoring

Monitoring is a new application in Information platform services 4.0. This application provides the ability to capture the runtime and historical metrics of Information platform services 4.0 servers, for reporting and notification. The monitoring application helps system administrators to identify if an application is functioning normally and if the response times are as expected. By providing key business metrics, the monitoring application provides better insight into Information platform services 4.0.

Monitoring allows you to:

- Check the performance of each server: This is possible with the help of watches, which show the state of each server as traffic lights. The system administrator can set thresholds for these watches and receive alerts when these thresholds are breached. This helps in taking proactive action if there is an impending failure or outage.
- View critical system Key Performance Indicators (KPIs): This helps in activity and resource monitoring. These KPIs are displayed on the dashboard page of the monitoring application.
- Check system availability and response time: Using probes, you can simulate workflows to check if the servers and services in the Enterprise deployment are functioning as expected. By analyzing the roundtrip time of these probes at periodic intervals, the system administrator can assess the system usage pattern.
- Analyze peak load and peak period for the CMS: This helps the system administrator determine if more licenses or system resources are required.
- Integrate with other enterprise applications: The Information platform services 4.0 monitoring application can be integrated with other enterprise applications like SAP Solution Manager and IBM Tivoli Monitoring.

## 13.2 Monitoring terms

The following list provides terms that relate to the monitoring application:

### **Dashboard**

The Dashboard page provides a centralized view for the system administrator to monitor the performance of all servers. It provides real-time information on the system KPIs, recent alerts, watches, and corresponding graphs based on the watch state.

**Watch**

Watches provide real-time status and historical trends of servers and workflows within the Information platform services environment. Users can associate thresholds and alerts to a watch. You can create a watch using data from probes, servers, SAPOSCOL or Derived Metrics.

**Derived Metrics**

Derived metric gives you the flexibility to create metrics based on the user's requirements, and then create a watch using this metric. You can create a derived metric by combining two or more existing metrics in a mathematical equation.

**KPI**

KPIs (key performance indicators) are standard metrics in the Information platform services deployment. They provide information about the schedules and log on sessions. For example, a higher number of **RunningJobs** indicates good performance of the servers. Alternatively, a higher number of **PendingJobs** indicates poor performance and high system load.

**Probes**

Probes monitor different services and simulates the different functionalities of Information platform services components. By scheduling probes to run at specified intervals, the system administrator can track the availability and performance of key services provided by Information platform services 4.0. This data can also be used for capacity planning.

**Traffic lights**

Traffic lights represent the watch state at any given time. The colors Green, Amber, and Red are used to indicate the state of a watch. Users can choose to set two or three states to a watch.

**Trending graph**

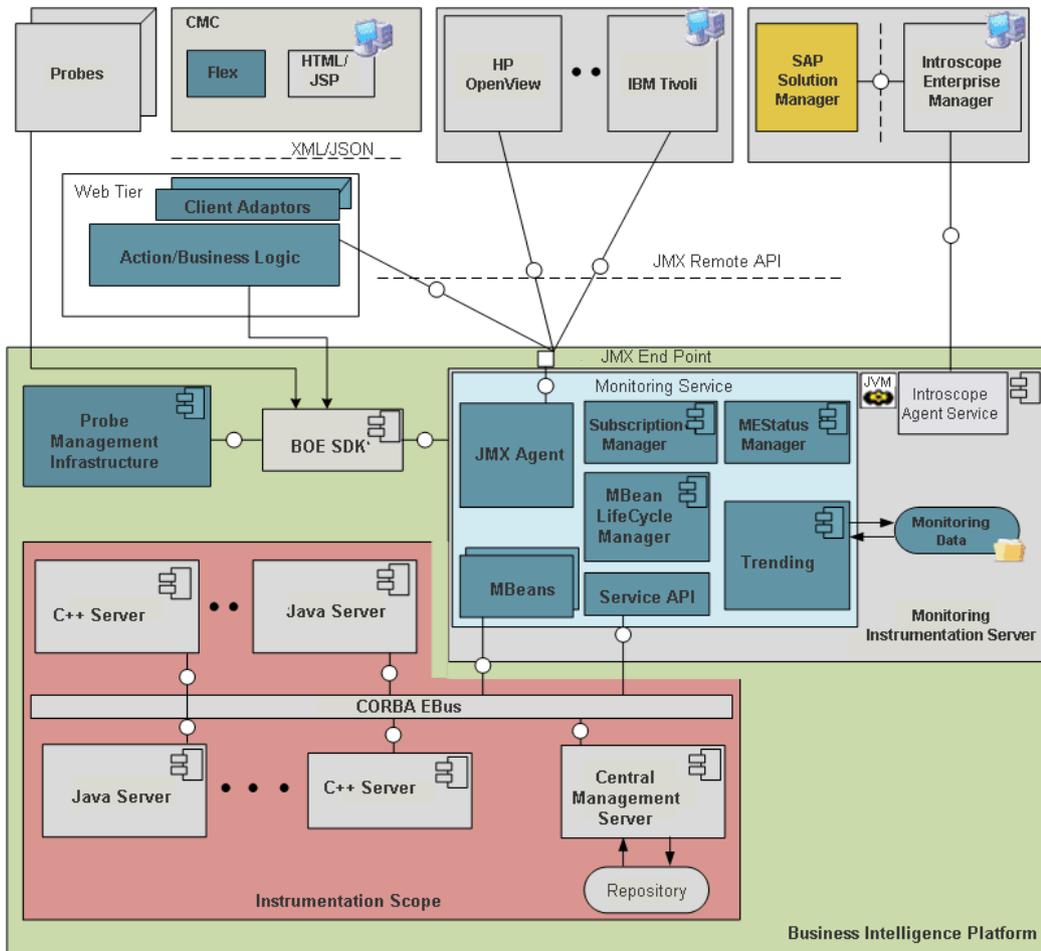
A trending graph is a graphical representation of historical metric data generated by probes and servers. It helps the system administrator monitor the system at different time intervals, and assess the system usage pattern.

**Alert**

An alert is a notification generated by the monitoring application, when a user-defined threshold value set for different metrics applied to a watch is breached. You can choose to receive alerts either through email or view on the "Dashboard" page.

## 13.2.1 Architecture

This section provides a high-level overview of the monitoring architecture and briefly explains the roles the components play. The monitoring architecture is represented graphically below:



The high-level components in the architecture are listed below:

- The Platform Java Server (PJS)
- The Java Management Extensions (JMX) agent/server
- MBeans
- JMX Clients
- The Management consoles
- Trending Database

The monitoring service is hosted on the Platform Java Server. The application is based on JMX technology.

The Monitoring Platform Java Service provides the core services available in the monitoring application. The Monitoring Platform Java Service provides the following services:

- Provides the JMX agent service.
- Creates MBeans dynamically for the SAP BusinessObjects servers.
- Provides lifecycle management for the MBeans.
- Provides a mechanism for registering new probes.
- Allows users to create complex threshold conditions using the metrics of the servers.

- Provides a threshold notification mechanism and sends alerts.
- Provides a trending function by storing historical data.

The Probe Scheduling Service that is hosted on the Adaptive Job Server manages the running and scheduling of probes. Hence, the Adaptive Job Server should be running for the probes to run.

The monitoring application also exposes a JMX or Remote Method Invocation (RMI) URL end point. Other enterprise applications such as SAP Solution Manager and IBM Tivoli Monitoring can connect to the monitoring application and access the SAP BusinessObjects metrics by using a JMX Remote API. The monitoring application uses a dedicated Derby database for storing historical data for the purpose of trending. For information on the trending database schema, see [Trending DB schema](#).

### 13.2.1.1 Trending DB schema

The following Trending Database diagram and table explanations show you the tables where the metric, probe, and watch data will be recorded and how these tables are related.

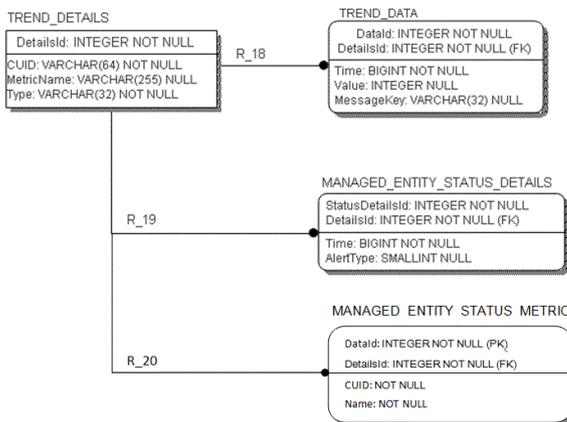


Table 13-1: TREND\_DETAILS

This table records information about managed entities, probes, and watches. For example, CUID and metric names.

Column name	Description	Primary key
DetailsId		Autogenerated
CUID (64)	CUID of the InfoObject (or) the unique id of non-InfoObject	NOT NULL
MetricName	Name of the Metric	NOT NULL
Type (32)	Subscription or Metric types	NOT NULL

Table 13-2: TREND\_DATA

This table records the trending data from metrics, watches, and probes. For example, metric value and time.

Column name	Description	Primary key
DataId		Auto generated
DetailsId		Foreign key
Time	Time at which data was collected	NOT NULL
Value	Value of the metric / subscription	No

Table 13-3: MANAGED\_ENTITY\_STATUS\_DETAILS

This table records the information about subscription breaches and alert delivery information. For example, breach time and alert delivery time.

Column name	Description	Primary key
StatusDetailsId		Auto generated
DetailsId		Foreign key
Time	Time at which data was collected	NOT NULL
AlertType	Subscription notification delivery type (for example, email)	No

### 13.3 Cluster support for monitoring server

The monitoring application provides cluster support. The cluster support is easy to implement and provides failover support.

With cluster support, only one service will be active at any given time, and all other services will be passive. Let us assume there are two monitoring services s1 and s2 in a clustered environment. Only one of them must be available. Both s1 and s2 attempt to become active. Only one of them will be successful and the other service becomes inactive or passive.

The passive services keep checking on a periodic basis (every one minute) on the availability of the active service. If the active service is unavailable, the passive service immediately attempts to become active.

**Note:**

It is recommended that the monitoring service is hosted on a separate AdaptiveProcessingServer (APS) instance to avoid crash or restart or poor performance of the APS.

## 13.4 Metrics

There are many metrics that can be used for creating watches. Metrics can be:

- Probe metrics
- Server metrics
- Host metrics
- Derived metrics

When a default probe is run, the metrics `execution time` and `passed` are generated. These metrics are called virtual metrics.

The Information platform services 4.0 server metrics are listed in the following table:

Server	Metrics
Adaptive Processing Server	<ul style="list-style-type: none"> <li>• Auditing Events Received</li> <li>• AuditingMetrics.number of Events in the Queue</li> <li>• Available Processors</li> <li>• Busy Server Threads</li> <li>• CPU Usage Percentage</li> <li>• Cube Count</li> <li>• CvomServerImpl.debugClassID</li> <li>• DataFederatorService.activeConnectorsConnectionsCount</li> <li>• DataFederatorService.activeConnectorsCount</li> <li>• DataFederatorService.activeQueriesCount</li> <li>• DataFederatorService.activeThreadsCount</li> <li>• DataFederatorService.analyzingQueriesCount</li> <li>• DataFederatorService.connectionsCount</li> <li>• DataFederatorService.diskUsedSize</li> <li>• DataFederatorService.executingQueriesCount</li> <li>• DataFederatorService.failedQueriesCount</li> <li>• DataFederatorService.memoryUsedSize</li> <li>• DataFederatorService.metadataCacheSize</li> <li>• DataFederatorService.optimizingQueriesCount</li> <li>• DataFederatorService.outputDataTransfer</li> <li>• DataFederatorService.outputRowsCount</li> <li>• DataFederatorService.queriesConsumingMemoryCount</li> <li>• DataFederatorService.queries UsingDiskCount</li> <li>• DataFederatorService.sourceInputDataTransfer</li> <li>• DataFederatorService.sourceInputRowsCount</li> <li>• DataFederatorService.waitingQueriesCount</li> <li>• Failed extraction attempts since the service start</li> <li>• Free Memory</li> <li>• JVM Deadlocked Threads Counter</li> <li>• JVM Lock Contention Count</li> <li>• Maximum Memory</li> <li>• Number of Full GCs</li> <li>• Number of Page Faults during GC</li> <li>• Percentage of stopped system during GC</li> <li>• Query Count</li> <li>• Server Enabled State</li> <li>• Server Running State</li> <li>• Session Count</li> <li>• Successful extraction attempts since the service start</li> <li>• Threads in Transport Layer</li> <li>• Total Memory</li> <li>• Transport Layer Thread Pool Size</li> </ul>

Server	Metrics
Central Management Server	<ul style="list-style-type: none"> <li>• Auditing Thread Utilization</li> <li>• Average Commit Response Time Since Startup (msec)</li> <li>• Average Query Response Time Since Startup (msec)</li> <li>• Busy Server Threads</li> <li>• CPUs</li> <li>• Completed Jobs</li> <li>• Currently Used System Database Connections</li> <li>• Disk Size (GB)</li> <li>• Established System Database Connections</li> <li>• Existing Concurrent User Accounts</li> <li>• Existing Named User Accounts</li> <li>• Failed Jobs</li> <li>• Longest Commit Response Time since Startup (msec)</li> <li>• Longest Query Response Time Since Startup (msec)</li> <li>• Number of Commits since Startup</li> <li>• Number of Objects in CMS System Cache</li> <li>• Number of Objects in CMS System DB</li> <li>• Number of Queries since Startup</li> <li>• Number of Sessions Established by All Users</li> <li>• Number of Sessions Established by Concurrent Users</li> <li>• Number of Sessions Established by Named Users</li> <li>• Number of Sessions Established by Servers</li> <li>• Number of User Logons Since Startup</li> <li>• PID</li> <li>• Peak Number of User Sessions Since Startup</li> <li>• Pending Jobs</li> <li>• Pending System Database Request</li> <li>• RAM (MB)</li> <li>• Running Jobs</li> <li>• Server Enabled State</li> <li>• Server Pending State</li> <li>• Used Disk Space (GB)</li> <li>• Waiting Jobs</li> <li>• Auditing Database Last Updated On</li> <li>• Auditing Thread Last Polling Cycle Duration (sec)</li> <li>• CMS Auditor</li> <li>• Concurrent User Licenses</li> <li>• Connection to Auditing Database is Established</li> <li>• Current Number of Auditing Events in Queue</li> <li>• Named User Licenses</li> </ul>
Event Server	

Server	Metrics
	<ul style="list-style-type: none"><li>• Busy Server Threads</li><li>• CPUs</li><li>• Disk Size (GB)</li><li>• Monitored Files</li><li>• PID</li><li>• RAM (MB)</li><li>• Server Enabled State</li><li>• Server Running State</li><li>• Used Disk Space (GB)</li><li>• Current Number of Auditing Events in the Queue N Pseudoloc</li></ul>
Input File Repository	<ul style="list-style-type: none"><li>• Active Connections</li><li>• Active Files</li><li>• Available Disk Space in Root Directory (%)</li><li>• Available Disk Space in Root Directory (GB)</li><li>• Busy Server Threads</li><li>• CPUs</li><li>• Data Sent (MB)</li><li>• Data Written (MB)</li><li>• Disk Size (GB)</li><li>• Free Disk Space in Root Directory (GB)</li><li>• PID</li><li>• RAM (MB)</li><li>• Server Enabled State</li><li>• Server Running State</li><li>• Total Disk Space in Root Directory (GB)</li><li>• Used Disk Space (GB)</li></ul>

Server	Metrics
Output File Repository	<ul style="list-style-type: none"> <li>• Active Connections</li> <li>• Active Files</li> <li>• Available Disk Space in Root Directory (%)</li> <li>• Available Disk Space in Root Directory (GB)</li> <li>• Busy Server Threads</li> <li>• CPUs</li> <li>• Data Sent (MB)</li> <li>• Data Written (MB)</li> <li>• Disk Size (GB)</li> <li>• Free Disk Space in Root Directory (GB)</li> <li>• PID</li> <li>• RAM (MB)</li> <li>• Server Enabled State</li> <li>• Server Running State</li> <li>• Total Disk Space in Root Directory (GB)</li> <li>• Used Disk Space (GB)</li> </ul>
PM Repository Server	<ul style="list-style-type: none"> <li>• Busy Server Threads</li> <li>• CPUs</li> <li>• Disk Size</li> <li>• PID</li> <li>• RAM</li> <li>• Server Enabled State</li> <li>• Server Running State</li> <li>• Used Disk Space</li> </ul>
Web Application Container Server	<ul style="list-style-type: none"> <li>• Server Enabled State</li> <li>• Server Running State</li> </ul>

## 13.5 Configuration properties

This section describes the monitoring application properties and how you can edit them.

To see the configuration properties of the monitoring application:

1. Go to the **Applications** area of the CMC.
2. Right-click **Monitoring** and select **Properties**. The "Monitoring Application Properties" window appears. The configurable properties are described in the following table:

Section	Field	Description
	<b>Enable Monitoring Application</b>	Select this option to enable monitoring functionalities. If you deselect this option, all monitoring functions except probes will be disabled. Probe trending will also be disabled.
	<b>Default JMX agent end point URL (IIOp)</b>	This contains the default JMX agent end point URL that uses IIOp protocol. This URL is generated automatically if you enable monitoring and then restart the server. This is the default protocol for monitoring service. This is a read-only field.
RMI	<b>Enable RMI protocol for JMX</b>	By default, this option is disabled. If you enable this option, you must provide the RMI port number. This port will be used for both RMI registry entry and RMI connector port. This port should be available for the service; otherwise the service will fail to start. After you provide the RMI port number, restart the server. Once the server is restarted, the RMI JMX agent end point URL is generated. This is a read-only property containing the JMX agent's end point URL using RMI protocol. Use this URL to connect to monitoring from other clients.
Host Metrics	<b>Enable host metrics</b>	By default, this option is disabled. If you enable this option, you must provide the path to your installation of SAPOSCOL binary  To enable host metrics, you need to install SAPOSCOL.

Section	Field	Description
Other settings	<b>Metric Refresh Interval (seconds)</b>	<p>The minimum interval that you can specify is 15 seconds. This interval governs the following:</p> <ul style="list-style-type: none"> <li>Subscription computation of the watches: The caution and danger rules are computed continuously with an interval of time mentioned here.</li> <li>Calculating the watch state: Watch state is computed continuously with an interval of time mentioned in the metric refresh period if the Event setting of the watch is selected with the following option: <b>Change the watch state every time caution or danger evaluates to true.</b></li> <li>Trending period: History mode for the graphs is always trended continuously with an interval of time mentioned here.</li> </ul>
	<b>Delete older data when the database size grows more than ( MB)</b>	Data from trending database will be cleaned up when the database size exceeds the amount specified. A 30% buffer is created for the database. For example, if you have set this as 100 MB, and if the database has grown more than 100 MB when the system checks, the database will be cleared till 70 MB.
	<b>Monitoring UI auto refresh interval (seconds)</b>	This interval will be used in the monitoring user interface (including the dashboard, watch list, and probes) for auto refresh. Minimum interval is 15 seconds. Auto-refresh does not affect the time duration in Live mode in graphs, which is set to 15 seconds by default.
	<b>Run database cleanup task everyday at</b>	The database cleanup task starts at the time specified. The database will be cleaned when the database size exceeds the specified maximum amount.
	<b>Backup trending database</b>	By default, this option is disabled. If you enable this option, the trending database backup task starts at the time specified.
	<b>Trending database backup directory</b>	By default, the location is not specified. You can specify a location; however, provide an absolute path and not a relative path. In case of a shared location, permission should be given to access the shared location.
	<b>Run database backup tasks</b>	

Section	Field	Description
		The database backup task starts when you click this option. Specify the database backup directory location before choosing this option.
	<b>Trending database location</b>	By default, the trending database location is <INSTALL_DIR>\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. You can also specify a different location; however, provide an absolute path and not a relative path. For a clustered environment, the location can be shared and permission should be given to access the shared location.

3. Click **Save**.

**Note:**

When you change any of these properties except enabling and disabling the monitoring application, you must restart the monitoring service that is hosted on the Adaptive Processing Server.

### Installing SAPOSCOL

Perform the following steps to install SAPOSCOL:

1. Download SAPHOSTAGENT710\_XX.SAR from SAP Marketplace (<http://service.sap.com>).
2. Extract SAPHOSTAGENT710\_XX.SAR by executing the `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR` command.
3. Install `saphostexec` by executing the `saphostexec.exe -install` command. Once `saphostexec` is installed as a service, SAPOSCOL is started.
4. Check SAPOSCOL status by executing the `saposcol -s` command.

## 13.5.1 JMX end point URL

The monitoring application exposes a JMX end point URL through which other clients can connect using JMX Remote API. By default, the JMX connectivity is provided over the IIOP (Internet Inter-Orb Protocol) or CORBA (Common Object Request Broker Architecture) transport. This connection URL is displayed in the properties page of the monitoring application. Being able to connect over IIOP absolves the need to worry about firewalls and having to expose ports. The CORBA ports are available by default. The jar files listed in the following table are needed at the JMX client end to be able to connect:

Jar Files
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wSDL4J-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

Another option is to connect through the default RMI port. For more information on how to connect through the RMI port, see [Configuration properties](#).

## 13.6 Integrating with other applications

Enterprise solutions, such as SAP Solution Manager and IBM Tivoli Monitoring, integrate with the monitoring application as JMX clients connecting via the JMX end point URL. After integration, the SAP BusinessObjects metrics can be viewed from the Client's user interface.

### 13.6.1 Integrating the monitoring application with IBM Tivoli

To integrate monitoring application with IBM Tivoli, you need to create, install, and configure an IBM Tivoli Monitoring Agent. Perform the following steps to create an IBM Tivoli Monitoring Agent:

1. Install the IBM Tivoli Monitoring Agent builder version 6.2.1 software.
2. Create a new agent. For information on how to create a new agent, see the IBM Tivoli Monitoring Agent user's guide.
3. In the Defining data monitoring types step, select Data from a server in the **Monitoring Data Categories** area and select JMX in the **Data Sources** area.
4. Click **Next**.
5. In the "JMX Information" window, click **Browse** to see all the JMX MBeans on the MBean server.

**Note:**

If you are running the browser for the first time, you need to add a new connection.

6. In the "Java Management Extensions (JMX) Browser" window, click + next to the **Connection Name** to add a new connection.
7. In the "MBean Server Connection Wizard" window, select Standard JMX Connections (JSR-160).
8. In the "Connection Properties" window, provide the following information:

Field	Description
Connection Name	JSR-160-Compliant Server
User ID	The username that is used to log into Information platform services
Password	The password that is used to log into Information platform services
Service URL	Provide the JMX endpoint URL

9. Click **Finish**.
10. In the **MBean Key Properties** area, select Domain and Type.  
All the MBeans appear in the text field below.
11. Select all the MBeans with domain as Servers, one MBean at a time such that the attributes are listed. Choose a key attribute if there is a possibility of having multiple MBeans of same type. For example, if there are two instances of a server running, then the PID of each instance can be a key attribute.
12. Select a server and select options for the JMX attribute group in the "JMX Agent-Wide Options" window.

13. In the "Data Source Definition" window, select the agent you added and click **Add to Selected**. This will take you to the beginning of the agent creation cycle and you need to repeat the above steps to add another server to be monitored.
14. After creating the agent, you need to install the agent. For more information on how to install an agent, see the IBM Tivoli Monitoring Agent user's guide Figure no. 154 onwards. This section gives information about installing the agent locally and also about creating an installable solution of the agent.

**Note:**

If you are creating an agent for Information platform services using the Agent Builder, then you need to have Information platform services 4.0 installed on the same system. However, if you are installing an already created agent using its installer file, then you do not need to have BOE monitoring installed because at configuration time you can give the details of any system with a JMX end point.

Perform the following steps to configure an installed agent:

1. Open "Manage Tivoli Enterprise Monitoring Services" in TEMS Mode. You will see the agent installed.
2. Right-click the agent template and select **Configure using defaults**.
3. Select an instance name.

The agent can be configured by using two different protocols: RMI and BOEIIOP.

To use RMI protocol:

- Click **Next**. Do not make any changes to the Java parameters.
- Provide values for JMX credentials, such as User ID, Password, and Service URL. For more information, see *Configuration Properties* in the Related Topics.
- Click **OK**.

To use BOEIIOP protocol:

- Copy `bcm.jar` and `cryptojFIPS.jar` files from `%InstallDir%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` to a folder in your system.
- Copy the jar files listed in the following table to another folder.
- In the Java parameters, set JVM arguments to `-Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring` and `-Djmx.boeiiop.bcm.dir=< folder location where you have copied bcm.jar and cryptojFIPS.jar files`.
- Select **Next**.
- Provide values for JMX credentials, such as User ID, Password, and Service URL. For more information, see *Configuration Properties* in the Related Topics.
- Set **<Jar Directories>** value as the location of the folder where you copied the list of jar files provided in the table.
- Click **OK**.

Jar files
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

4. Right-click the agent and select **Start** in the "Manage Tivoli Enterprise Monitoring Services" window.
5. Open IBM Tivoli Enterprise Portal Desktop/Browser Client. A button appears on the "Navigator" window.
6. Click the Navigator button.

The agent is added to the Navigator.

### Related Topics

- [Configuration properties](#)

## 13.6.2 Integrating the monitoring application with SAP Solution Manager

To integrate the monitoring application with SAP Solution Manager, you need to have [Wily Introscope](#) installed and running in your system. The SAP Solution Manager must be configured for Introscope workstation. Perform the following steps during Information platform services 4.0 installation:

1. In the Configure Connectivity to Introscope Enterprise Manager step, provide the host name and port details. An Introscope Agent will be installed at `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley` when Information platform services 4.0 is installed.
2. Launch Introscope workstation and click **New Investigator**. You can view the SAP BusinessObjects server metrics and probe virtual metrics in the JMX section of the agent configured.

**Note:**

You can configure the Introscope (IS) agent by choosing **CMC > Servers > Server node > Placeholders**. The IS Enterprise Manager host and port are also configured here for the IS agent to communicate with the monitoring application. For more information, see *Managing Servers* in the *SAP BOE CMC Help* guide.

For the JMX metrics to be available in IS, ensure that both the IS agent services and monitoring service are available on the AdaptiveProcessingServer Instance.

If you enable IS instrumentation, the code instrumentation gets enabled automatically.

## 13.7 Creating Universe for Derby Database

You create a universe for Derby database in order to run queries in the Derby database to create reports and perform data analysis. For more information on creating universes, refer to the *SAP BOE Universe Designer* guide.

**Note:**

You create a universe for Derby database only after you run backup tasks for the database. For more information on database backup tasks, see *Configuration Properties* in the Related Topics.

1. Create a universe for Derby database by running the Universe Design Tool wizard.  
For more information on creating universe using the wizard, see *Using the Quick Design Wizard* in the *SAP BOE Universe Designer* guide.  
You can create the universe using two database connections, Apache and Generic.
2. If you select Apache connection, proceed as follows:
  - a. Click **JDBC Drivers**
  - b. Select the `derby.sbo` file from the location `<INSTALL_DIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc`.

- c. Add the classpath `<ClassPath> <Path> \... \... \derby.jar</Path></ClassPath>`.  
Download the latest `derby.jar` file (version 10.5.x) from the Apache website before adding the classpath.
  - d. To create a new Apache database connection, enter the Derby database folder location in the **Server** field.  
If the database is located in `C:\Derby`, enter `C:\Derby;create=false`
3. If you select Generic connection, proceed as follows:
- a. Select **Generic JDBC Datasource**.
  - b. Select the `jdbc.sbo` file from the location `<INSTALL_DIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc`.
  - c. Add the classpath `<ClassPath> <Path> \... \... \derby.jar</Path></ClassPath>` and JDBC class details `<Parameter Name="JDBC Class">org.apache.derby.jdbc.EmbeddedDriver</Parameter>`
  - d. If you are creating a new Generic database connection, enter `jdbc:derby:C:\Derby;create=false` in the **URL** field

#### Related Topics

- [Configuration properties](#)

## 13.8 Troubleshooting

This section provides step -by-step solutions to a wide range of problems that may occur in your work with the monitoring application.

### 13.8.1 Dashboard

#### Monitoring link is not displayed on the CMC page

- Check if the user has adequate access rights.
- Ensure that the user is added to the Monitoring User or Administrator group or to any other group that is a part of these groups.

#### Key Performance Indicators (KPIs) are not visible on the Monitoring Dashboard

- Check if the required metrics are visible by choosing **CMS Server properties > Metrics**.
- Ensure that the Central Management Server is responding as expected.

**Unable to launch the monitoring application**

Download and install the latest Flash player (10.5.x).

## 13.8.2 Alerts

**Unable to receive alerts on the Alerts page**

- Check if the **Enable Alert Notification** in the **Notification** settings is selected
- Ensure that you have adequate access rights to receive alerts
- Check if the recent alerts are visible on the monitoring dashboard
- Check if the SMTP server is functioning
- Check if the e-mail ID set to receive e-mail alerts is appropriate
- Ensure that AdaptiveJobServer instance is enabled
- Check the SMTP settings in the AdaptiveJobServer instance destination

**Note:**

You can send a CR document to the e-mail ID you set to test if the SMTP is working as expected.

## 13.8.3 Watchlist

**Unable to receive historical data for Watch**

- Check for polling interval on the monitoring application **Properties** page
- Check the trace file in the logging folder
- Check if the **Trending database location** is specified on the CMC **Applications** page. For a clustered environment, ensure that the user has permissions to access the shared location. For more information, see *Configuration Properties* in the Related Topics.
- Check if the system time of the server and client is the same in a specific time zone

**An error occurred while retrieving synchronized live data**

Check if the AdaptiveProcessingServer instance is running.

**Watchlist tab is disabled**

- Check if the server, to which the metric is assigned, is running
- Check if the corresponding metric in the metric list page displays the information in live and historical modes
- Check the monitoring service logs for error messages
- Check if the metric is visible in the jconsole

**Related Topics**

- [Configuration properties](#)

**13.8.4 Probes****Unable to schedule Probes**

- Check if the AdaptiveJobServer instance is running
- Ensure that the report CUID, that is used for Crystal reports and Web Intelligence documents, is appropriate
- Ensure that the user has administrative rights or is a member of the Administrator group
- Check if the user has adequate rights to open, refresh, export Crystal Reports or Web Intelligence documents that are used in the corresponding probes

**Probe schedule status is "pending"**

- Check if the ProbeSchedulingService instance is installed
- Check if the AdaptiveJobServer instance is running

**An error occurred while retrieving the trend data from the database**

Check if the AdaptiveProcessingServer is running.

**probeRun.bat fails to run successfully**

- Check if `java_home` is set
- Check if the correct parameters are entered in the command prompt

**Note:**

Enter `probeRun.bat -help` in the command prompt to check if all the parameters are appropriate

**13.8.5 Metrics****Host metrics are not listed**

- Ensure that SAPOSCOL is running
- Ensure that the **Enable Host Metrics** option is selected on the monitoring application **Properties** page
- Restart the AdaptiveProcessingServer instance for the changes to be effective
- Ensure that **Path to your installation of SAPOSCOL binary** is appropriate

**Error occurred while retrieving JMX Client**

Check if the AdaptiveProcessingServer instance is running.

**SAPOSCOL metric value is zero on the Metric page**

- Ensure that SAPOSCOL is running
- Execute the following on the host where SAPOSCOL is installed:
  1. `saposcol -s` to check the status
  2. `saposcol -m` to get a snapshot of the data collected by SAPOSCOL

## **13.8.6 Graph**

**Graphs show different times for the live and history modes**

Ensure that the system time of the server and client is the same in a specific time zone.

**Graph data is not displayed in history mode for a cluster scenario**

Ensure that all the AdaptiveProcessingServer instances point to the same Derby database location.

# Auditing

## 14.1 Overview

Auditing allows you to keep a record of significant events on servers and applications, which helps give you a picture of what information is being accessed, how it's being accessed and changed, and who is performing these operations. This information is recorded in a database called the Auditing Data Store (ADS). Once the data is in the ADS, you can design custom reports to suit your needs. You can look for sample universes and reports on the [SAP Developer Network](#).

For the purposes of this chapter, an auditor is a system responsible for recording or storing information on an event, and an auditee is any system responsible for performing an auditable event. There are some circumstances where a single system can perform both functions.

### How Auditing works

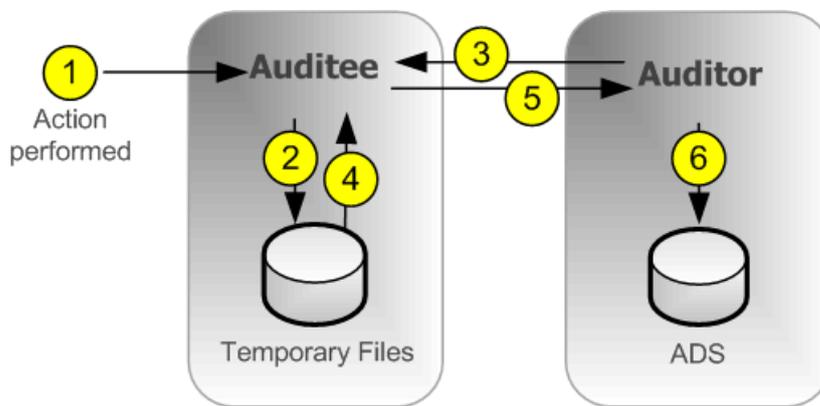
The Central Management Server (CMS) acts as the system auditor, while each server or application that triggers an auditable event acts as an auditee. When an audited event is triggered, the auditee will generate a record and store it in a local temporary file. At regular intervals, the CMS communicates with the auditees to request these records and writes the data to the ADS.

The CMS also controls the synchronization of auditing events that occur on different machines. Each auditee provides a timestamp for the auditing events that it records. To ensure that the timestamps of events on different servers are consistent, the CMS periodically broadcasts its system time to the auditees. The auditees then compare this time to their internal clocks. If differences exist, they correct the time recorded for subsequent auditing events.

Depending on the type of auditee, the system uses one of the following workflows to record the events.

### Server auditing

In cases of server generated events, the CMS can act as both Auditee and Auditor.

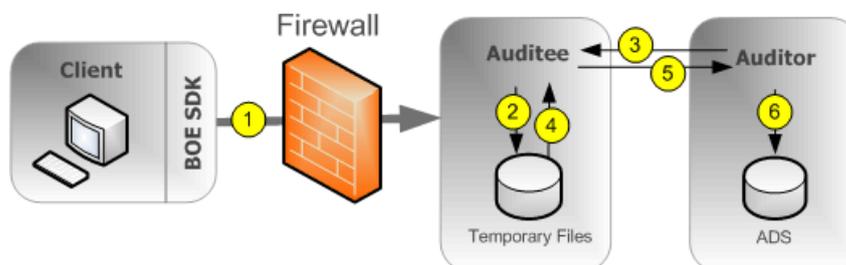


NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

1. An auditable event is performed by the server.
2. The server auditee writes events in a temporary file.
3. The auditor polls the auditee and requests a batch of auditing events.
4. The server auditee retrieves the events from the temporary files.
5. The server auditee transmits the events to the auditor.
6. The auditor writes events to the ADS and signals the server auditee to delete the events from the temporary files.

#### Client logon auditing for clients connecting through CORBA

This includes applications such as SAP BusinessObjects Web Intelligence.



NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

1. The client connects to the CMS, which will act as the auditee. The client provides its IP address and machine name, which the auditee then verifies.

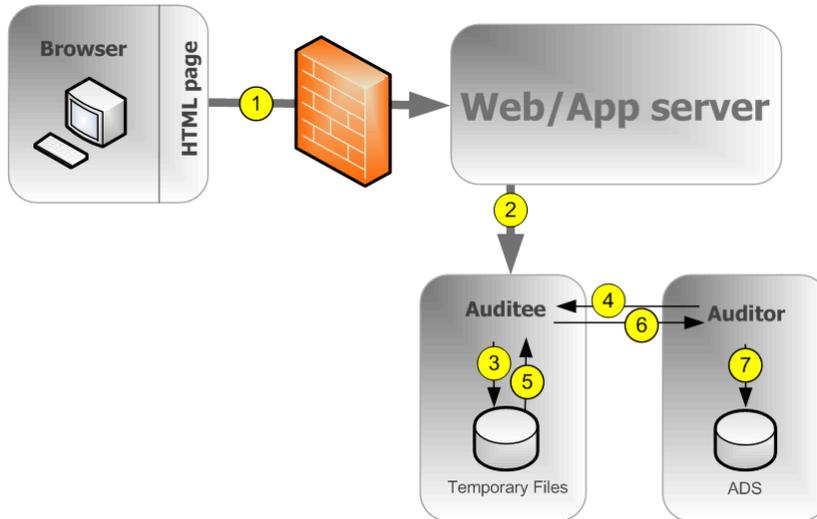
**Note:**

A port should be opened in the firewall between the client and CMS. More details on firewalls can be found in the security chapter of the *Information platform services Administrator's Guide*.

2. The auditee writes events in a temporary file.
3. The auditor polls the auditee and requests a batch of auditing events.
4. The auditee retrieves the events from the temporary files.
5. The auditee transmits the events to the auditor.
6. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

### Client logon auditing for clients connecting through HTTP

This includes online applications such as BI launch pad, Central Management Console, Web Intelligence, and so on.

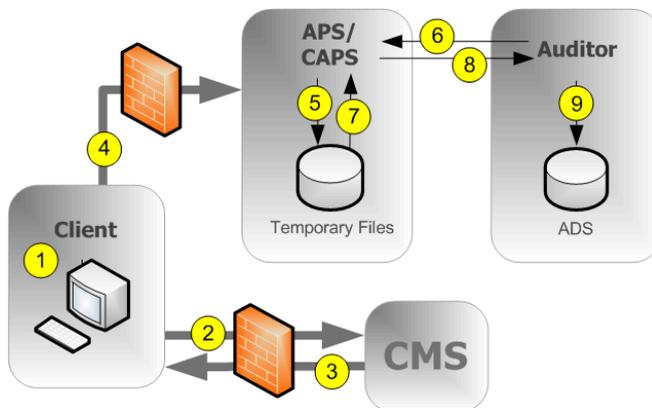


NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

1. The browser connects to the web application server, and logon data is submitted to the web application server.
2. Information platform services SDK submits the logon request to the auditee (CMS), along with the IP address and name of the browser machine.
3. The auditee writes events in a temporary file.
4. The auditor polls the auditee and requests a batch of auditing events.
5. The auditee retrieves the events from the temporary files.
6. The auditee sends events to the auditor.
7. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

### Non-logon auditing for clients connecting through CORBA

This workflow applies to auditing Web Intelligence events when connecting through CORBA.



1. The user performs an operation that may be audited.
2. The client contacts the CMS to check if the operation is configured to be audited.
3. If the action is set to be audited, the CMS communicates this information to the client.
4. The client sends the event information to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server.

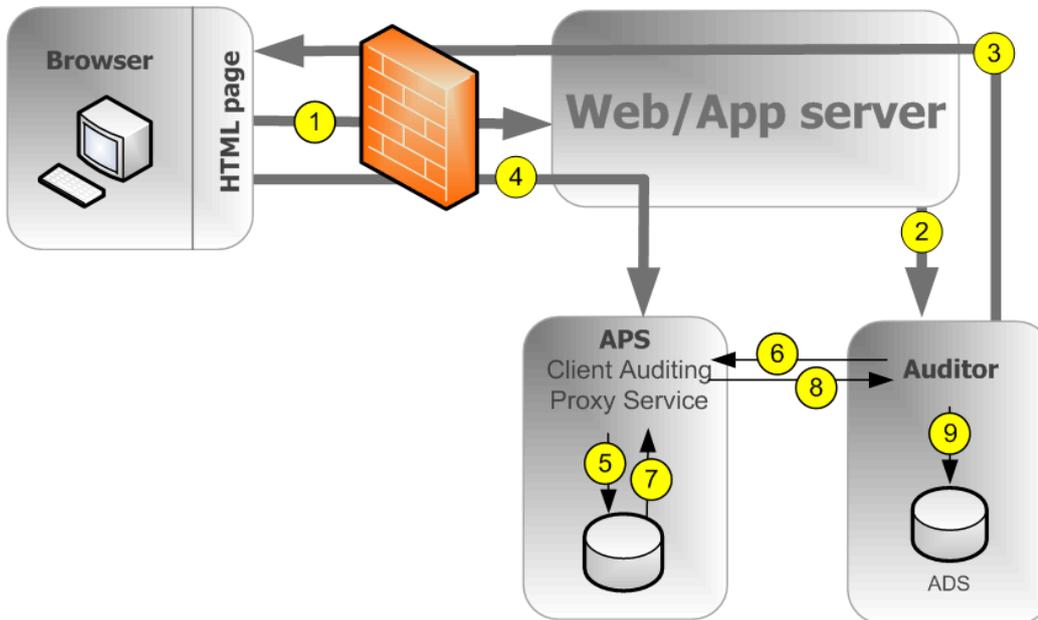
**Note:**

A port in the firewall should be opened between each client and any Adaptive Processing Servers that hosts a CAPS, and also between each client and the CMS. More details on firewalls can be found in the security chapter of the *Information platform services Administrator's Guide*.

5. The CAPS writes events in a temporary file.
6. The Auditor polls the CAPS and requests a batch of auditing events.
7. The CAPS retrieves the events from the temporary files.
8. The CAPS sends the event information to the auditor.
9. The auditor writes events to the ADS and signals the CAPS to delete the events from the temporary files.

**Non-login auditing for clients connecting through HTTP**

This workflow applies to auditing Web Intelligence 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 checks to see if the event is configured to be audited.

**Note:**

The diagram shows the Auditor CMS being contacted, but any CMS in the cluster can be contacted for this information.

3. The CMS returns the audit configuration information to the web application server, which passes this information back to the client application.
4. If the event is configured to be audited, the client sends the event information to the web application server, which passes it to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server (APS).
5. The CAPS writes events in a temporary file.
6. The auditor polls the CAPS and requests a batch of auditing events.
7. The CAPS retrieves the events from the temporary files.
8. The CAPS sends the event information to the auditor.
9. The auditor writes events to the ADS and signals the CAPS to delete the events from the temporary files.

**Clients that support auditing**

The following client applications support auditing:

- Central Management Console (CMC)
- BI launch pad
- Open Document
- Analysis
- Live Office Web Services Provider

- Web Intelligence desktop

**Note:**

At least one instance of CAPS must be running in order to collect auditing events from the clients listed above.

Clients not listed above do not directly generate events, but some actions performed by the servers as a result of client application operations can be audited.

**Auditing consistency**

In most cases, where auditing is properly installed, configured, secured, and correct versions of all client applications are used, auditing will properly and consistently record all indicated system events. It is important to keep in mind, however, that certain system and environment conditions can adversely affect auditing.

There is always a delay between the time an event occurs and its final transfer to the Auditor database. Conditions such as the unavailability of the CMS or auditing database or loss of network connectivity can increase these delays.

As a system administrator, you should work to avoid any of the following conditions, which could result in incomplete auditing records:

- A drive where auditing data is stored reaches maximum capacity. You should ensure plenty of disk space is available for your auditing database and auditee temporary files.
- An auditee server is improperly removed from the network before it can transmit all audit events. You should ensure that when removing a server from the network, sufficient time is allowed for audit events to post to the auditing database.
- The deletion or modification of auditee temporary files.
- A hardware or disk failure.
- Physical destruction of an auditee or auditor host machine.

In the following scenarios, audit events may be prevented from reaching the CMS-Auditor:

- Users with older client versions.
- Transmission of auditing information may be blocked by improperly configured firewalls.

**Note:**

- Events generated by client applications contain information submitted from the client side, in other words outside the trusted area of the system. Therefore under some conditions this information may not be as reliable as information recorded by the system servers. This also includes events generated by the BI workspaces Cache Server, since this server sits outside the trusted area.
- If you want to remove a server from your deployment, you should first disable that server but keep it running and connected to your network until all the events in the temporary files have had a chance to transfer to the auditing database. The server's "Current Number of Auditing Events in the Queue" metric will show how many auditing events are waiting to be transferred, when this reaches zero you can stop the server. The location of the Temporary files is defined in the **Placeholders** for that node. See the Server Administration chapter for more details on placeholders.
- If you will use Client Auditing, create a dedicated Adaptive Processing Server for the Client Auditing Proxy Service to ensure best system performance. To increase your system's fault tolerance, consider running the CAPS on more than one APS.

**Related Topics**

- [Server and node placeholders](#)

**14.2 CMC Auditing page**

The "Auditing" page in the CMC has the following areas:

- "Auditing Status Summary"
- "Set Events"
- "Set Event Details"
- "Configuration"

**14.2.1 Auditing Status Summary**

The "Auditing Status" Summary shows a set of metrics that help you optimize your auditing configuration and alert you to any issues that might affect the integrity of your auditing data. The status summary is at the top of the "Auditing" page in the Central Management Console.

The summary will also display warnings under the following circumstances:

- The connection to the Auditing Data Store (ADS) database is unavailable.
- There is no running or enabled Client Auditing Proxy Service, which prevents client events from being collected.
- An auditee has events that could not be retrieved (the server or servers affected will be identified). This usually indicates a server was not properly stopped or shut down and still has events in the temporary files.

**Auditing status metrics**

<b>Metric</b>	<b>Details</b>
ADS Last Updated on	The date and time the auditor CMS last started polling the auditees for their auditing events.
Auditing Thread Utilization	<p>The percentage of the polling cycle the auditor CMS spends collecting data from auditees, the remainder is time spent resting between polls.</p> <p>If this reaches 100% the figure will be displayed in yellow, and means the auditor is still collecting data from the auditees when the next poll is due to begin. This may cause delays in the events reaching the ADS.</p> <p>If this is happening frequently or persistently, it is recommend you either update your deployment to allow the ADS database to receive data at a higher rate (faster network connections or more powerful database hardware for example), or decrease the number of auditing events your system tracks.</p>
Last Polling Cycle Duration	<p>Duration of the last polling cycle in seconds. This indicates the maximum delay for event data to reach the ADS during the previous polling cycle.</p> <ul style="list-style-type: none"> <li>• If the duration is under 20 minutes (1200 seconds), the figure appears on a green background.</li> <li>• If the duration is between 20 minutes and two hours (7200 seconds), it appears on a yellow background.</li> <li>• If the duration is over two hours, it appears on a red background.</li> </ul> <p>If this state persists and you consider the delay too long, either update your deployment to allow the ADS database to receive data at a higher rate (faster network connections or more powerful database hardware for example) or decrease the number of auditing events that your system tracks.</p>
CMS Auditor	The name of the CMS currently acting as auditor.
ADS Database Connection Name	The name of the database connection currently used by the auditor CMS to connect to the Auditing Data Store (ADS). For SQL Anywhere and HANA servers, it is the name of the ODBC connection. For other database types, it is the server name, connection port, and database name.
ADS Database User Name	The user name the auditor CMS is using to log on to the ADS database.

## 14.2.2 Configuring Auditing events

The CMC Auditing page can be used to activate auditing and select which events will be audited across your entire system.

If you are not interested in certain events or event details, you can leave them unselected to gain additional system performance.

**Note:**

If you chose not to configure your ADS connection when you installed Information platform services, you will need to set up a connection to the database before you configure your auditing events. See *Auditing Data Store configuration settings*.

### 14.2.2.1 To configure auditing events

1. In the Central Management Console, click the **Auditing** tab.  
The "Auditing" page appears.
2. Set the **Set Events** slider to the desired level.  
The following table shows the four different settings for the slider and the events captured at each level.

Auditing Level	Events captured
<b>Off</b>	None
<b>Minimal</b>	<ul style="list-style-type: none"> <li>• Logon</li> <li>• Logout</li> <li>• Rights Modification</li> <li>• Custom Access Level Modified</li> <li>• Auditing Modification</li> </ul>
<b>Default</b>	<b>Minimal</b> events, plus: <ul style="list-style-type: none"> <li>• View</li> <li>• Refresh</li> <li>• Prompt</li> <li>• Create</li> <li>• Delete</li> <li>• Modify</li> <li>• Save</li> <li>• Search</li> <li>• Edit</li> <li>• Run</li> <li>• Deliver</li> </ul>
<b>Complete</b>	<b>Minimal</b> and <b>Default</b> events plus: <ul style="list-style-type: none"> <li>• Retrieve</li> <li>• Trigger</li> <li>• Drill Out of Scope</li> <li>• Page Retrieved</li> <li>• LCM Configuration</li> <li>• Rollback</li> <li>• VMS Add</li> <li>• VMS Retrieve</li> <li>• VMS Check-in</li> <li>• VMS Check-out</li> <li>• VMS Export</li> <li>• VMS Lock</li> <li>• VMS Unlock</li> <li>• Cube Connection</li> <li>• MDAS Session</li> </ul>
<b>Custom</b>	You select a custom set of events.

3. If you selected **Custom**, click the events you want to capture on the list below the **Set Events** slider.
4. Under "Set Event Details," click the optional details you want to record with the events.  
Recording fewer details will increase system performance.

Detail	Description
<b>Query</b>	If set, "Query" event detail (Detail ID 25) will be recorded for any event that queries a database.
<b>Folder Path Details</b>	If set, the following details will be captured: <ul style="list-style-type: none"> <li>• "Object Folder Path (Detail ID 71)"</li> <li>• "Top Folder Name (Detail ID 72 "</li> <li>• " Container folder path (Detail ID 64)"</li> </ul>
<b>Rights Details</b>	If set, the following details will be captured: <ul style="list-style-type: none"> <li>• "Right Added (Detail ID 55)"</li> <li>• "Right Removed (Detail ID 56)"</li> <li>• "Right Modified (Detail ID 57)"</li> </ul>
<b>User Group Details</b>	If set, the following details will be captured: <ul style="list-style-type: none"> <li>• " User Group Name (Detail ID 16)"</li> <li>• "User Group ID (Detail ID 15)"</li> </ul>
<b>Property Value Details</b>	If set, the "Property Value" event detail (Detail ID 29) will be captured when the properties of an object are updated. This is generated only for CMC, BI launch pad or SharePoint events.

5. Click **Save**.

**Note:**

For client auditing, it may take up to two minutes after the changes have been made before the system will start recording data for any new events. Make sure you allow for this delay when implementing changes to the system.

### 14.2.3 Auditing Data Store configuration settings

If you chose not to set up an auditing database when you installed Information platform services, or you want to change the database location or settings, you can use the following steps to configure the connection to the ADS.

This is also where you can configure how long auditing events will be retained in the database.

If you have performed an upgrade from a previous version of Information platform services XI 3.x and have installed version 3.x of Business Objects Metadata Manager (BOMM), it is recommended to configure the ADS to use the same database or tablespace as BOMM.

**Note:**

If you are using an existing DB2 9.7 Workgroup as the auditing database then ensure that the database account is configured to have a page size over 8 kB.

### 14.2.3.1 To configure your Auditing Data Store database settings

1. On the Central Management Console, select the **Auditing** tab.  
The **Auditing** page appears.
2. Under the "Configuration" heading, click **ADS Database Type**.  
A list of supported database types appears.
3. Select the database type you have set up for your auditing data.
4. Under **Connection Name**, enter the name of the connection you have configured for the auditing database. For SQL databases this will be the ODBC name; all other databases will take the form `<serverhostname>, <port>, <databasename>`.
  - a. If you are using an Microsoft SQL database with Windows authentication, enable the **Windows Authentication** option.
5. In the **User Name** and **Password** fields, enter the user name and password you want the auditor CMS to use when logging onto the database.
6. In the **Delete events older than (days)** field, enter the number of days you want information to remain in the database. (Minimum value 1, maximum value 109,500.)

**Caution:**

Data older than the number of days set here will be permanently deleted from the ADS; it cannot be recovered. You may want to consider periodically moving records to an archive database if you want to maintain long-term records.

7. In the event the database connection is lost, if you want to manually reconnect the auditor-CMS to the database, de-select the **ADS Auto Reconnect** option.

**Note:**

If this is unchecked, you will need to manually re-establish a connection to the ADS if the connection is lost. This can be done by restarting the CMS, or enabling **ADS Auto Reconnect**. Events will be recorded and remain stored in the temporary files until the ADS is reconnected.

8. Click **Save**.
9. Restart the CMS.

## 14.3 Audit events

The following table shows all the auditing events in the system, and gives a brief description for each. A list of the service types that create the events follows.

Event	Description and servers and clients that generate the event type
Auditing Modification	<p>The system's auditing settings are modified.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> </ul>
Create	<p>A new object is added to the system.</p> <ul style="list-style-type: none"> <li>• Web Intelligence Processing Service</li> <li>• Crystal Reports Viewing and Modification Service</li> <li>• Central Management Service</li> <li>• Web Intelligence</li> <li>• Lifecycle Management</li> </ul>
Cube Connection	<p>An OLAP Cube Connection operation is performed.</p> <ul style="list-style-type: none"> <li>• Multi-Dimensional Analysis Service</li> </ul>
Custom Access Level Modified	<p>Information for privileges are modified.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> </ul>
Delete	<p>An object is removed from the system.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> <li>• Lifecycle Management Service</li> </ul>
Deliver	<p>An object is sent/delivered to a destination.</p> <ul style="list-style-type: none"> <li>• Destination Delivery Scheduling Service</li> <li>• Crystal Reports Scheduling Service</li> <li>• Crystal Reports for Enterprise Scheduling Service</li> <li>• Web Intelligence Publishing and Scheduling Service</li> <li>• Central Management Service</li> <li>• Program Scheduling Service</li> </ul>
Drill out of scope	<p>A user of a Web Intelligence document has drilled down to a detail level outside the report's pre-loaded data.</p> <ul style="list-style-type: none"> <li>• Web Intelligence</li> <li>• Web Intelligence Processing Service</li> </ul>
Edit	<p>The content of an object is changed.</p> <ul style="list-style-type: none"> <li>• Web Intelligence Processing Service</li> <li>• Dashboard Service</li> <li>• Web Intelligence</li> </ul>
LCM Configuration	<p>The configuration details of Lifecycle Management Console (LCM) are changed.</p> <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>
Logon	<p>A user logs onto the system.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> </ul>

Event	Description and servers and clients that generate the event type
Logout	<p>A user logs out of the system.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> </ul>
Modify	<p>The file properties of an object are changed.</p> <ul style="list-style-type: none"> <li>• Web Intelligence</li> <li>• Lifecycle Management</li> <li>• Central Management Service</li> </ul>
MDAS Session	<p>A multidimensional analysis services operation is performed</p> <ul style="list-style-type: none"> <li>• Multi-Dimensional Analysis Service</li> </ul>
Page Retrieved	<p>An SAP BusinessObjects Web Intelligence client retrieves additional information from the repository.</p> <ul style="list-style-type: none"> <li>• Web Intelligence Processing Service</li> </ul>
Prompt	<p>Information is entered for a object prompt.</p> <ul style="list-style-type: none"> <li>• Dashboards Cache Service</li> <li>• Live Office</li> <li>• Crystal Reports Scheduling Service</li> <li>• Crystal Reports for Enterprise</li> <li>• Crystal Reports Cache Service</li> <li>• Web Intelligence Processing Service</li> <li>• Web Intelligence</li> </ul>
Refresh	<p>The data in an object is updated from the database at a user's request.</p> <ul style="list-style-type: none"> <li>• Dashboards Cache Service</li> <li>• Live Office</li> <li>• Crystal Reports for Enterprise Scheduling Service</li> <li>• Crystal Reports Cache Service</li> <li>• Crystal Reports Scheduling Service</li> <li>• Web Intelligence Processing Service</li> <li>• Web Intelligence</li> </ul>
Retrieve	<p>An object is retrieved from the repository.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> </ul>
Rights Modification	<p>The security information is changed for a user, group, or object.</p> <ul style="list-style-type: none"> <li>• Central Management Service</li> </ul>
Rollback	<p>LifeCycle Manager is used to revert an object to a previous version.</p> <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>

Event	Description and servers and clients that generate the event type
Run	<p>A job is run.</p> <ul style="list-style-type: none"> <li>• Lifecycle Management Scheduling Service</li> <li>• Destination Delivery Scheduling Service</li> <li>• Replication Service</li> <li>• Crystal Reports Scheduling Service</li> <li>• Crystal Reports for Enterprise Scheduling Service</li> <li>• Web Intelligence Scheduling and Publishing Service</li> <li>• Publication Scheduling Service</li> <li>• Program Scheduling Service</li> <li>• Lifecycle Management</li> </ul>
Save	<p>An object is saved after being updated or changed.</p> <ul style="list-style-type: none"> <li>• Crystal Reports Enterprise Scheduling Service</li> <li>• Crystal Reports Cache Service</li> <li>• Multi-Dimensional Analysis Service</li> <li>• Lifecycle Management Service</li> <li>• Web Intelligence Processing Service</li> <li>• Crystal Reports Viewing and Modification Service</li> <li>• Crystal Reports Scheduling Service</li> </ul>
Search	<p>A search is performed.</p> <ul style="list-style-type: none"> <li>• Search Service</li> </ul>
Trigger	<p>A file event is triggered.</p> <ul style="list-style-type: none"> <li>• Event Service</li> <li>• Central Management Service</li> </ul>
View	<p>An object is Viewed.</p> <ul style="list-style-type: none"> <li>• Web Intelligence</li> <li>• Web Intelligence Processing Service</li> <li>• Central Management Console</li> <li>• BI Launch Pad</li> <li>• Dashboards Cache Service</li> <li>• Crystal Reports Cache Service</li> <li>• Crystal Reports Viewing and Modification Service</li> <li>• Dashboard Service</li> <li>• OpenDocument</li> </ul>
VMS Add	<p>An object is added to the LCM Version Management System.</p> <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>
VMS Check in	<p>An object is checked into the LCM Version Management System.</p> <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>

Event	Description and servers and clients that generate the event type
VMS Check out	An object is checked out of the LCM Version Management System. <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>
VMS Export	A resource is exported from the VMS. <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>
VMS Lock	A resource in the VMS is locked. <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>
VMS Unlock	A resource in the VMS is unlocked. <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>
VMS Retrieve	An object is retrieved from the LCM Version Management System. <ul style="list-style-type: none"> <li>• Lifecycle Management</li> </ul>

#### Events by service-type

Service type	Event types generated
Authentication Update Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Run</li> </ul>
BI Launch Pad	View
Central Management Service	<ul style="list-style-type: none"> <li>• Auditing Modification</li> <li>• Create</li> <li>• Custom Access Level Modified</li> <li>• Delete</li> <li>• Deliver</li> <li>• Logon</li> <li>• Logout</li> <li>• Modify</li> <li>• Retrieve</li> <li>• Rights Modification</li> <li>• Trigger</li> </ul>
Central Management Console	View
Crystal Reports 2011 Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Prompt</li> <li>• Refresh</li> <li>• Run</li> <li>• Save</li> </ul>

Service type	Event types generated
Crystal Reports Cache Service	<ul style="list-style-type: none"> <li>• Prompt</li> <li>• Refresh</li> <li>• Save</li> <li>• View</li> </ul>
Crystal Reports for Enterprise Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Prompt</li> <li>• Refresh</li> <li>• Run</li> <li>• Save</li> </ul>
Crystal Reports Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Prompt</li> <li>• Refresh</li> <li>• Run</li> <li>• Save</li> </ul>
Crystal Reports Viewing and Modification Service	<ul style="list-style-type: none"> <li>• Create</li> <li>• Save</li> <li>• View</li> </ul>
Dashboards Cache Service	<ul style="list-style-type: none"> <li>• Prompt</li> <li>• Refresh</li> <li>• View</li> </ul>
Dashboard Applications	<ul style="list-style-type: none"> <li>• Edit</li> <li>• View</li> </ul>
Destination Delivery Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Run</li> </ul>
Event Service	Trigger
Information Engine Service	<ul style="list-style-type: none"> <li>• Create</li> <li>• Drill out of scope</li> <li>• Edit</li> <li>• Page retrieved</li> <li>• Prompt</li> <li>• Refresh</li> <li>• Save</li> <li>• View</li> </ul>
LCM Scheduling Service	Run

Service type	Event types generated
LCM service	<ul style="list-style-type: none"> <li>• Create</li> <li>• Delete</li> <li>• LCM console configuration</li> <li>• Modify</li> <li>• Rollback</li> <li>• Run</li> <li>• Save</li> <li>• VMS Add</li> <li>• VMS Checkin</li> <li>• VMS Checkout</li> <li>• VMS Delete</li> <li>• VMS Export</li> <li>• VMS Lock</li> <li>• VMS Retrieve</li> <li>• VMS Unlock</li> </ul>
Live Office	<ul style="list-style-type: none"> <li>• Prompt</li> <li>• Refresh</li> </ul>
Multi-Dimensional Analysis Service	<ul style="list-style-type: none"> <li>• MDAS Cube Connection</li> <li>• MDAS Session</li> <li>• Save</li> </ul>
OpenDocument	View
Platform Search Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Run</li> </ul>
Platform Search Service	Search
Probe Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Run</li> </ul>
Program Scheduling Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Run</li> </ul>
Publication Scheduling Service	Run
Replication Service	Run
Security Query Scheduling Service	<ul style="list-style-type: none"> <li>• Run</li> <li>• Deliver</li> </ul>
Users and Groups Import Scheduling Service	<ul style="list-style-type: none"> <li>• Run</li> <li>• Deliver</li> </ul>

Service type	Event types generated
Visual Difference Scheduling Service	Run
Web Intelligence Application	<ul style="list-style-type: none"><li>• Create</li><li>• Drill out of scope</li><li>• Edit</li><li>• Modify</li><li>• Page retrieved</li><li>• Prompt</li><li>• Refresh</li><li>• Save</li><li>• View</li></ul>
Web Intelligence Common Service	<ul style="list-style-type: none"><li>• Create</li><li>• Drill out of scope</li><li>• Edit</li><li>• Page retrieved</li><li>• Prompt</li><li>• Refresh</li><li>• Save</li><li>• View</li></ul>

Service type	Event types generated
Web Intelligence Core Service	<ul style="list-style-type: none"> <li>• Create</li> <li>• Drill out of scope</li> <li>• Edit</li> <li>• Page retrieved</li> <li>• Prompt</li> <li>• Refresh</li> <li>• Save</li> <li>• View</li> </ul>
Web Intelligence Processing Service	<ul style="list-style-type: none"> <li>• Create</li> <li>• Drill out of Scope</li> <li>• Edit</li> <li>• Page Retrieved</li> <li>• Prompt</li> <li>• Refresh</li> <li>• Save</li> <li>• View</li> </ul>
Web Intelligence Scheduling and Publishing Service	<ul style="list-style-type: none"> <li>• Deliver</li> <li>• Run</li> </ul>

### Event properties and details

Each event that is recorded by Information platform services XI includes a set of event properties and details.

Event properties will always be generated with an event, although some may not have values if the information is not applicable to a specific event. In the ADS, event properties are included in the table that stores the event, so they can be used to sort or group events when you create reports.

Event details record additional information about the event that is not included in the event's properties. If an event detail is not relevant to a specific event, that event detail will not be generated. There is a set of common event details that can be generated for all event types when they are relevant. There are also sets of additional event details which are generated for specific event types. For example, Prompt events record the values entered for the prompt in an event detail, but no other event type generates a prompt value event detail. In the ADS, details are stored on a separate table which is linked to the parent event.

Any multilingual data (such as object or folder names) will be recorded in the default language for the locale of the auditor CMS.

### 14.3.1 Audit events and details

The following sections list the event types, followed by a description of any properties and event details that are unique to those events.

**Note:**

Some client programs do not have their own unique events and rely on the common and platform events to capture relevant information about their operations.

#### 14.3.1.1 Universal event properties and details

The following tables show what properties and event details are recorded for all events.

Event property	Description
Event_ID	A unique identifier for the event.
Client_Type_ID	Identifier for the type of application that performed the event
Service_Type_ID	Shows the ID of the type of service or application that triggered the event.
Start_Time	The start date and time when the event started (in GMT).
Duration	Duration of the event in milliseconds.
Session_ID	ID of the session during which the event was triggered.
Event_Type_ID	Type of event (for example, 1002 for view).
Status_ID	Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events.
Object_ID	<p>CUID of the object affected (if applicable). CUID of the alerting event for Trigger events.</p> <p><b>Note:</b> All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client computer for example. You will need to use the Object_Name property to differentiate these objects.</p>
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.

Event property	Description
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, <code>Sales/North America/East Coast</code>
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in <code>Sales/North America/East Coast</code> then the value would be <code>Sales</code> .
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in <code>Sales/North America/East Coast</code> then the value would be the CUID of the folder <code>Sales</code> .
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.
Parent Document ID	12	<ul style="list-style-type: none"> <li>For a document instance: the CUID of the parent document.</li> <li>For parent documents: its own CUID.</li> </ul>
Universe ID	13	CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used.

Event Detail	ID	Description
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups, an event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups, an event detail will be generated for each group.

### 14.3.1.2 Common events

The following event types are common to all SAP BusinessObjects XI servers and clients.

#### View

User viewed a document / object.

- Event Type ID: 1002

Event detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

#### Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. <b>Note:</b> For View on Demand Crystal Reports this will be set to 0.
Number of Rows	63	The number of records the database server returned. <b>Note:</b> For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.
Publication Instance ID	37	ID of this instance of the publication. Only applicable to publishing workflows.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents.

**Prompt**

A value was entered for a prompt.

- Event Type ID: 1004

Event detail	ID	Description
Prompt name	26	The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a document or object, and they will be grouped.
Prompt value	27	The value entered for a prompt. A separate detail will be generated for each value entered. These can be grouped together and related back to the prompt name.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).
Publication Instance ID	37	ID of this instance of the publication. Only applies to publishing workflows.
Name at Design Time	90	The name of the Xcelsius document at the time it was designed. This is only generated for Xcelsius refreshes, or an Xcelsius or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

### Create

User created an object.

- Event Type ID: 1005

Event detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Overwrite	21	Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable.
Description	24	Records any information in the document or object's description field.

### Delete

User deleted an object.

- Event Type ID: 1006

## Modify

User modified a file property or the file properties of an object.

- Event Type ID: 1007

Event detail	ID	Description
Property Name	28	The name of the property that was modified. An event detail will be generated for each modified property.
Property Value	29	The new value for any modified property of the document or object. An event detail will be generated for each modified property.

## Save

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed
  - "2" indicates the object was successfully saved or exported to a repository
  - "3" indicates the object was successfully saved or exported to a new format

Event detail	ID	Description
Size	17	Size of the object (in bytes) that was saved or exported.
File Name	18	The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension (for example, doc for a Microsoft Word file or pdf for an Adobe PDF file).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable. .

## Search

A search was conducted.

- Event Type ID: 1009

Event detail	ID	Description
Keyword	19	The keywords of the conducted search.
Category	20	Category used in the search (if applicable).
Number of Rows	63	The number of rows returned by the search.

### Edit

User edited the content of an object.

- Event Type ID: 1010

Event detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Query	25	If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.)
Universe Object Name	31	The name of the universe the document or object uses. A separate detail will be generated for each universe accessed by the document or object.
Container ID	32	The CUID of the container (a dashboard for example) that uses the object (if applicable).
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

### Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be attempted again
  - "3" indicates the job was cancelled

Event detail	ID	Description
Size	17	Size of the document (in bytes) that was run.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

### Deliver

An object was delivered.

- Event Type ID: 1012

Event detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable).
From address	41	Records the sender's address for documents/objects distributed by email (if applicable).
To address	42	Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient.
File Name	18	Records the file name of documents/objects distributed by email or FTP, or written directly to a disk that is not part of the Business Objects deployment.

Event detail	ID	Description
Account Name	45	This records one of the following: <ul style="list-style-type: none"> <li>For <b>Inbox</b> delivered objects, a list of BusinessObjects user account names.</li> <li>For <b>FTP</b> delivered objects, the FTP account name.</li> <li>For <b>Unmanaged Disk</b> delivered objects, the login account used.</li> <li>For <b>SMTP</b> delivered objects, the login account used for the SMTP server.</li> </ul>
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	35	Indicates how the delivery was initiated: <ul style="list-style-type: none"> <li>"0" indicates scheduled</li> <li>"1" indicates sent to a destination</li> <li>"2" indicates published</li> <li>"3" indicates an alert was triggered</li> </ul>

### Retrieve

An object is retrieved from the CMS.

- Event Type ID: 1013

### Logon

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt
  - "2" indicates a named-user license logon was successful
  - "3" indicates a non-user (system) login was successful

Event detail	ID	Description
Concurrent User Count	50	The number of users on the system at the time the event was triggered.
Hostname reported by client	51	Hostname of client as reported by client.
Hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value will be recorded.
IP address reported by client	53	IP address of client as reported by the client.
IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value will be recorded.

### Logout

A user logs off.

- Event Type ID: 1015

Event detail	ID	Description
Concurrent User Count	50	The number of concurrent users on the system at the time the event was triggered.

### Trigger

A file event is triggered.

- Event Type ID: 10016

Event detail	ID	Description
File Name	17	The name of the file that was being monitored and triggered the event.

## 14.3.1.3 Platform events

The following events are specific to the Information platform services platform.

### Rights modification

Right or rights for an object were modified.

- Event Type ID: 10003

Event Detail	ID	Description
Rights Added	55	The type of right added, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: <code>added right=Export; new value=Granted; scope=Current object; applicable object type=all object types.</code>
Rights Re-removed	56	The type of right removed, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: <code>removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types.</code>
Rights Modified	57	The type of right modified, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: <code>modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types.</code>

#### Custom Access Level modified

A Custom Access Level was modified.

- Event Type ID: 10004

Event Detail	ID	Description
Rights Added	55	The type of right added, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: <code>added right=Export; new value=Granted; scope=Current object; applicable object type=all object types</code>
Rights Re-removed	56	The type of right removed, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example : <code>removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types.</code>
Rights Modified	57	The type of right modified, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example : <code>modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types.</code>

#### Auditing modification

A change was made to the system's auditing settings.

- Event Type ID: 10006

Event Detail	ID	Description
Event Type ID	58	Records the ID of the auditing event type that was enabled or disabled. If multiple event types are enabled or disabled in one action, an event detail will be generated for each event type.
Action	59	Records which auditing events were enabled or disabled.
New Auditing Level	60	If the auditing level of detail is changed, records the new level setting (off, minimal, or default for example).
Old Auditing Level	61	If the auditing level of detail is changed, records the previous level setting (off, minimal, or default for example).
Auditing option	62	If an optional detail is enabled or disabled, the detail modified is recorded and whether it was enabled or disabled. If multiple details are enabled or disabled in a single action, a detail record will be generated for each modified detail.
ADS Connection	70	If the connection to the Auditing Data Store is changed, this records the new connection settings using the following format: <code>DBType=Oracle, DBName=MyADS, Username=USR1, Password="*****", SSO=off, DBReconnect=on</code> . Only the details changed will be recorded. For example, if the user name is the only thing updated, then only <code>Username="new"</code> will be recorded.  <b>Note:</b> The password information will always be obscured with * in the database.
Auto Delete Interval	105	This detail will record any changes to the <b>Delete Events Older Than</b> field in the Auditing CMC page. This governs how many days auditing information will be maintained in the ADS.

#### 14.3.1.4 Lifecycle management events

The following events are unique to the Lifecycle management for SAP BusinessObjects component.

##### Common details

All Lifecycle management events will have the following additional event details.

Event Detail	ID	Description
Element Cluster	6	The CUID of affected clusters when Lifecycle management console performs an operation on objects located in different clusters. An event detail will be generated for each affected cluster.
Element Comment	7	Additional information on the object.
Primary Element	8	If the element is a primary element, this detail will be set to "1"; if it is a dependent element, it will be set to "0".
Element Status	9	If the operation element fails this detail will be set to "1"; otherwise it will be "0".
Operation	10	Describes the type of operation performed (for example Add, Delete, or Modify).

### Configuration

Configuration of Lifecycle management is changed.

- Event Type ID: 10900

Event Detail	ID	Description
Configuration	100	A user views the Lifecycle management console configuration. The configuration displays as comma-separated value pairs, for example: rollback settings=enabled, port=900.
Configuration Before	101	If the Lifecycle management console settings for an object are modified, records the previous configuration settings. Uses the same format as Configuration.
Configuration After	102	If the Lifecycle management console settings for an object are modified, records the new configuration settings. Uses the same format as Configuration.
VMS Type	10900	The type of version management system.

### Rollback

An object was rolled back to a previous Version Management System (VMS) version.

- Event Type ID: 10901

### VMS Add

A resource is added to the VMS.

- Event Type ID: 10902

Event Detail	ID	Description
Version	104	Records the version number of the document in the Version Management System.

### VMS Retrieve

A resource is retrieved from the VMS.

- Event Type ID: 10903

Event Detail	ID	Description
Restore Deleted Object	103	Indicates if a retrieved object had been deleted from the system. "0" indicates the object was not deleted; "1" indicates the object was deleted.
Version	104	Records the version number of the document in the VMS.

### VMS Checkin

A resource is checked into the VMS.

- Event Type ID: 10904

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.

### VMS Checkout

A resource is checked out from the VMS.

- Event Type ID: 10905

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.

### VMS Export

A resource is exported from the VMS.

- Event Type ID: 10906

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.

**VMS Lock**

A resource in the VMS is locked, to prevent users editing it.

- Event Type ID: 10907

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.
Locked By	10901	The user name of the user who performed the action.

**VMS Unlock**

A resource in the VMS is unlocked, allowing users to edit it.

- Event Type ID: 10908

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.
Unlocked By	10901	The user name of the user who performed the action.



# Supportability

## 15.1 Logging traces from components

Tracing allows system administrators and support personnel to report on the performance of SAP BusinessObjects Enterprise components (servers and web applications) and the activity that occurs within the monitored components.

System-level messages generated by SAP BusinessObjects Enterprise servers are traced and written to log files. These log files are used by system administrators to monitor performance or for debugging purposes. Traces are recordings of events that occur during the operation of a monitored component. The traced events range from severe exception errors on one end to simple status messages at another.

### Trace Log

Trace messages are collected in log files saved under the generic log file (.glf) extension. In setting the trace log level for a component, you determine the type and verbosity of information sent to the log file. The trace log level is in effect a filter that suppresses traces that are below a specified importance level. Suppressed traces are not written to the output log file. By monitoring the trace log for a component, you can determine whether the current instance of a component or its configuration must be changed to handle the increased workload, or whether the increased load has no significant effect on the performance.

## 15.2 Trace log levels

The following table describes the available trace log levels for SAP BusinessObjects Enterprise components:

Level	Description
Unspecified	The trace log level is specified through another mechanism, usually an <code>.ini</code> file.
None	When the trace log level is set to "None", the filter to optionally suppress traces below a specified importance level is deactivated.  <b>Note:</b> A "None" trace log level does not mean that the tracing feature is turned off. System resources continue to be monitored and traces will be logged for rare critical events such as failed assertions.
Low	The trace log filter is set to allow for logging error messages while ignoring warning and most status messages. However, very important status messages will be logged for component startup, shutdown, as well as the start and end request messages.  <b>Note:</b> This level is not recommended for debugging purposes.
Medium	The trace log filter is set to include error, warning, and most status messages in the log output. Status messages that are least important or highly verbose will be filtered out. This level is not verbose enough for debugging purposes.
High	No messages will be excluded by the filter. This level is recommended for debugging purposes.  <b>Note:</b> A "High" trace log level could affect system resources. It could potentially increase CPU usage as well as storage space in the file system.

## 15.3 Configuring tracing for servers

Traces for a monitored SAP BusinessObjects Enterprise server are written to a specific log file (`.glf`) and stored in the Logging folder or directory. On Windows platforms the Logging directory is by default located in: `Program Files <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`. On Unix, the directory is located in: `<INSTALLDIR>/sap_bobj/logging`.

### **Note:**

The `.glf` file name is formatted as a combination of shorthand identifier, the server name, and number reference - for example `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. A new trace log file is created for the monitored server once the log file size approaches the one megabyte threshold.

Administrators are able to calibrate the severity and importance of the traces collected in the log file by setting the trace log level for a specific server or a collection of servers. You can modify the trace log level through the following recommended methods:

- Using the "TraceLog Service" for a specific server or a group of servers in the Central Management Console (CMC)
- Manually change the trace log level and other settings in the `BO_trace.ini` file.

If you want to only modify the trace log level for specific servers it is recommended that you use the "TraceLog Service" in the CMC. To modify other tracing parameters you must reconfigure the `BO_trace.ini` file.

### 15.3.1 To set the server trace log level in the CMC

The trace log level for a server can be adjusted without affecting other tracing settings. Follow the instructions below to adjust the trace log level.

1. Go to the "Servers" management area of the CMC.
2. Access the servers whose trace log level you want to modify.
  - a. Click the server category to access a server or servers from a specific server "category",
  - b. Click **Servers List** in the navigation pane to access the complete list of servers.
3. Right-click the server and select **Properties**.

The "Properties" dialog box is displayed.
4. In the "Trace Log Service" area, select the desired setting from the "Log level" list.
5. Click **Save & Close** to submit the modified trace log level.

The new trace log level will take effect within a minute.

To specify a different directory for the log files, use the `-loggingPath` parameter together with a path to the target directory in the "Command Line Parameters" area. This modification will not take effect until the server is restarted.

#### Related Topics

- [Trace log levels](#)

### 15.3.2 To set the trace log level for multiple servers managed in the CMC

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

The available Service Categories are displayed in the "Servers" page.
2. Access the servers whose trace log level you want to reset.
  - a. Click the server category to access a server or servers from a specific server category,.
  - b. Click **Server List** in the navigation pane to access the complete list of servers.

3. Select the servers.

To select multiple servers, hold down the **Ctrl** key while selecting.

4. Right-click and select **Edit Common Services**.

The "Edit Common Services" screen is displayed.

5. In the "Trace Log Service" area, select the desired setting from the "Log level" list.

6. Click **OK** to submit the modified trace log level.

The new trace log level will take effect within a minute.

To specify a different directory for the log files, use the `-loggingPath` parameter together with a path to the target directory in the "Command Line Parameters" area. This modification will not take effect until the servers are restarted.

### Related Topics

- [Trace log levels](#)

## 15.3.3 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, follow these steps:

1. Open the `BO_trace.ini` file.

- The default location on Windows is: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
- The default location on UNIX is: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.

2. Uncomment the required lines under the "Trace Syntax and Setting" section.

3. Modify the server tracing parameters as required.

The table below lists the general parameters used for configuring server tracing.

Parameter	Possible values	Description
active	false, true	If set to <code>true</code> , trace messages that meet the threshold set in the <code>importance</code> parameter will be traced. If set to <code>false</code> , trace messages will not be traced based on their "importance" level. Default value is <code>false</code> .
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl <b>Note:</b> importance = xs or importance = << are the most verbose options available while importance = xl or importance = >> are the least.	Specifies the threshold for tracing messages. All messages beyond the threshold will be traced. Default value is m (medium).
alert	false, true	If set to <code>true</code> , trace messages that meet the threshold set in the <code>severity</code> parameter will be traced. If set to <code>false</code> , the trace messages will not be traced based on their "severity" level. Default value is <code>true</code> .
severity	'S', 'W', 'E', 'A', 'F', success, warning, error, assert, fatal	Specifies the threshold severity over which messages can be traced. 'S' consumes the most disk space. 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_num	Possible values are integers >= 1000	Specifies the number of logs to keep.

Parameter	Possible values	Description
administrator	Strings or integers	Specifies an annotation to use in the output log file. The default value is blank. For example, if <pre>administrator = "hello"</pre> this string is inserted into the log file.
log_dir		Specifies the output log file directory. By default log files are stored in the Logging folder.
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.

#### 4. Save and close the BO\_trace.ini file.

The modified settings will not take effect until all the affected servers are restarted.

#### Example:

```
active=false;
severity='E';
importance='==';
size=1000000;
keep_num=437;
```

### 15.3.3.1 To configure tracing per server

The BO\_trace.ini file is used to specify tracing parameters for SAP BusinessObjects Enterprise servers. The settings affect all managed servers. Administrators can use the BO\_trace.ini file to set particular tracing parameters for a specific server.

#### 1. Open the BO\_trace.ini file.

- The default location on Windows is: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/.
- The default location on UNIX is: <INSTALLDIR>/sap\_bobj/enterprise\_xi40/conf/.

#### 2. Uncomment the required lines under the "Trace Syntax and Setting" section.

#### 3. To specify tracing settings for a specific server use an IF statement as shown in the example below:

```
if (process == "aps_MySIA.ProcessingServer")
{
    active = true;
    importance = '<<' ;
    alert = true;
    severity = ' ' ;
    keep_num = 487;
```

```
        size = 100 * 1000;  
    }
```

#### 4. Save and close the `BO_trace.ini` file.

The modified settings will be implemented with a minute. The new settings will override any trace log level specified in the CMC for a specific server.

## 15.4 Configuring tracing for web applications

Traces for a monitored SAP BusinessObjects Enterprise web application are written to a specific log file (`.glf`) and stored in a folder on the machine hosting the web applications folder. The trace log files will be located by default in the following directory: `$userHome/SBOPWebapp_$application_$IPaddress_$port/`

### Note:

On Windows, by default, Tomcat is installed and configured to run under the Local System account. `UserHome` is the root of the Windows drive (that is, `C:\`).

Administrators are able to calibrate the severity and importance of the traces collected in the log file by setting the trace log level for a specific or a collection of web applications. You can modify the trace log level through the following recommended methods:

- Using the "Trace Log" application settings in the Central Management Console (CMC)
- Manually reconfigure the trace log level and all other tracing settings in the `BO_trace.ini`. This file is deployed together with the `BOE` and `dswebobje` WAR files on your web application server.

To modify only the trace log level for a BOE web application, it is strongly recommended that you use the CMC option. To modify all tracing parameters you must reconfigure the `BO_trace.ini` file.

### Note:

Before reconfiguring the `BO_trace.ini` file, you must use the WDeploy tool to undeploy the existing web applications from your web application server. After reconfiguring `BO_trace.ini`, it must be redeployed together with the web applications on your web application server. For more information on using WDeploy to prepare, deploy, and undeploy web applications, see the *SAP BusinessObjects Enterprise Web Application Deployment Guide*.

### 15.4.1 To set the web application trace log level in the CMC

By default, the trace log level for web applications in the CMC is set to Unspecified. Trace log settings are available for the following applications in the CMC:

- Central Management Console

- BI launch pad
- Open Document
- Web Service
- Promotion Management
- Version Management
- Visual Difference

To trace all other web applications, manually configure the corresponding `BO_trace` file:

1. Go to the "Applications" management area of the CMC.  
The "Applications" page appears.
2. Right-click the application and choose **Trace Log Settings**.  
The "Trace Log Settings" page appears.
3. Select the desired setting in the **Log Level** list.
4. Click **Save & Close** to submit the trace log level.

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

#### **Related Topics**

- [Trace log levels](#)

## **15.4.2 To manually modify tracing settings through the `BO_trace.ini` file**

The `BO_trace.ini` file is deployed together with `BOE` and `dswsbobje` WAR files on the web application server. This file is not always accessible on the web application server. You must undertake the following preliminary step. The affected web application must be undeployed from the web application server.

1. Use `WDeploy` to undeploy the web application from your web application server. For more information on using `WDeploy` to undeploy web applications please see the *SAP BusinessObjects Enterprise Web Application Deployment Guide*.

#### **Note:**

If you are using the Tomcat web application server provided with the SAP BusinessObjects Enterprise installation, the `BO_trace.ini` file is accessible in the following directory. You do not need to undeploy the web applications and modify the file directly.

- The tracing configuration file for the `BOE.war` file is available at: `<INSTALLDIR>\Tomcat6\webapps\BOE\WEB-INF\TraceLog`.
- The tracing configuration file for the `dswsbobje.war` file is available at: `<INSTALLDIR>\Tomcat6\webapps\dswsbobje\WEB-INF\conf`.

If you are using the bundled Tomcat web application server skip to step 3.

2. Access a predeployed version of the `BO_trace.ini` file for the `BOE` or `dswsbobje` WAR files.

- A predeployed version of the configuration file for the `BOE.war` file is available by default in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
  - A predeployed version of the configuration file for the `dswsbobje.war` file is available by default in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.
3. Open the `BO_trace.ini` file.
    - The default location on Windows is: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf`.
    - The default location on UNIX is: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
  4. Uncomment the required lines under the "Trace Syntax and Setting" section.
  5. 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 <b>Note:</b> 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	'S', 'W', 'E', 'A', 'F', success, warning, error, assert, fatal	Specifies the threshold severity over which messages can be traced. 'S' consumes the most disk space. Default value is 'E'.
size	Possible values are integers $\geq$ 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
administrator	Strings or integers	Specifies an annotation to use in the output log file. The default value is blank. For example, if <pre>administrator = "hello"</pre> this string will be inserted into the log file.
log_dir		Specifies the output log file directory. By default log files are stored in the Logging folder.
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.

```
active=false;
severity='E';
importance='==';
size=1000000;
keep=false;
```

6. Save and close the `BO_trace.ini` file.
  7. Use WDeploy to deploy the WAR file on the machine hosting the web application server.
- The modified tracing settings take effect after the first log on to the web application.

### 15.4.2.1 To configure tracing for a specific web application

The `BO_trace.ini` file is used to specify tracing parameters for SAP BusinessObjects Enterprise web applications. The settings affect all the applications associated with the deployed WAR file. Administrators can also use the `BO_trace.ini` file to set particular tracing parameters for a specific web application.

In the current release of SAP BusinessObjects Enterprise, the table below lists the web applications and their associated WAR file.

Web application	WAR file	Predeployed location
Central Management Console	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
BI launch pad	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Open Document	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Web Service	dswsbobje.war	<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf

1. Use WDeploy to undeploy the web application from your web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Enterprise Web Application Deployment Guide*.

**Note:**

If you are using the Tomcat web application server provided with the SAP BusinessObjects Enterprise installation, the `BO_trace.ini` file is accessible in the following directory. You do not need to undeploy the web applications. You can modify the file directly.

- The tracing configuration file for the `BOE.war` file is available at: `<INSTALLDIR>\Tomcat6\webapps\BOE\WEB-INF\TraceLog`.
- The tracing configuration file for the `dswsbobje.war` file is available at: `<INSTALLDIR>\Tomcat6\webapps\dswsbobje\WEB-INF\conf`.

If you are using the bundled Tomcat web application server skip to step 3.

2. Access a predeployed version of the `BO_trace.ini` file for the `BOE` or `dswsbobje` WAR files.
  - A predeployed version of the configuration file for the `BOE.war` file is available by default in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
  - A predeployed version of the configuration file for the `dswsbobje.war` file is available by default in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.
3. Open the `BO_trace.ini` file.
4. Uncomment the required lines under the "Trace Syntax and Setting" section.
5. To specify tracing settings for a specific web application use an IF statement as shown in the example below:

```
if (device_name == "Webapp_opendocument_trace")
{
active = true;
importance = '<<' ;
alert = true;
severity = ' ';
keep_num = 332;
size = 100 * 1000;
}
```

The table below lists all the available parameters for configuring web application 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 <b>Note:</b> 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	'S', 'W', 'E', 'A', 'F', success, warning, error, assert, fatal	Specifies the threshold severity over which messages can be traced. 'S' consumes the most disk space. 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.
administrator	Strings or integers	Specifies an annotation to use in the output log file. The default value is blank. For example, if <pre>administrator = "hello"</pre> this string will be inserted into the log file.
log_dir		Specifies the output log file directory. By default log files are stored in the Logging folder.
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.

6. Save and close the BO\_trace.ini file.
7. Use WDeploy to deploy the WAR file on the machine hosting the web application server.

## 15.5 Configuring tracing for Upgrade management tool

Tracing for the Upgrade management tool is done via the `BO_trace.ini` configuration file .

The default location on Windows is: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.

The default location on Unix is: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.

**Note:**

Unlike other SAP BusinessObjects Enterprise components, tracing configuration for the Upgrade management tool cannot be performed via the CMC.

### 15.5.1 To configure tracing for Upgrade management tool

1. Open the `BO_trace.ini` file.
  - The default location on Windows is: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
  - The default location on UNIX is: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
2. Uncomment the required lines under the "Trace Syntax and Setting" section.
3. To specify tracing settings for a specific server use an IF statement as shown in the example below:

```
if (process == "upgrademanagementtool")
{
active = true;
importance = '<<' ;
alert = true;
severity = ' ';
keep = false;
size = 100 * 1000;
}
```

**Tip:**

The process must be specified as `upgrademanagementtool` for the tracing setting to apply to the Upgrade management tool.

4. Save and close the `BO_trace.ini` file.

The modified settings will be implemented with a minute.



# Command line administration

## 16.1 Command lines overview

This section lists the command-line options that control the behavior of each Information platform services server.

When you start a server through the Central Management Console (CMC) the server is started (or restarted) with a default command line that includes a typical set of options and values. In the majority of cases, you do not need to modify the default command lines. 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 in the CMC if you need to further customize the behavior of Information platform services.

Throughout this section, values provided in square brackets [ ] are optional.

**Note:**

The following tables list the supported command-line options. Information platform services servers use a number of internal options that are not listed in these tables. These internal options must not be modified.

### 16.1.1 To view or modify a server's command line

1. Use the Central Management Console (CMC) to stop the server.
2. Right-click the server and select **Properties**.
3. On the "Properties" screen, modify the command line for the server, and click **Save & Close**.
4. Start the server.

## 16.2 Standard options for all servers

These command-line options apply to all of the Information platform services servers, unless otherwise indicated. See the remainder of this section for options specific to each type of server.

Option	Valid Arguments	Behavior
<code>-requestPort</code>	<i>port</i>	<p>Specify the port that the server listens on. The server registers this port with the CMS. If unspecified, the server chooses any free port greater than 1024.</p> <p><b>Note:</b> When you change this port setting, it is the same as changing the <b>Request Port</b> field under "Common Settings" on a server's "Properties" page in the CMC.</p> <p><b>Note:</b> 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>Information Platform Services Administrator's Guide</i>.</p>
<code>-loggingPath</code>	<i>absolute path</i>	Specify the path where log files are created.

### 16.2.1 UNIX signal handling

On UNIX, the Information platform services 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).

### 16.3 Central Management Server

This section provides the command-line options that are specific to the CMS. The default path to the server on Windows is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

The default path to the server on Unix is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/boe_cmsd`.

Option	Valid Arguments	Behavior
<code>-threads</code>	<i>number</i>	Specifies the number of working threads that the CMS initializes and uses. The value can be between 12 and 150, and the default value is 50.
<code>-reinitializedb</code>		Cause the CMS to delete the system database and recreate it with only the default system objects. All existing data in the database is lost when it is recreated.
<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.

Option	Valid Arguments	Behavior
<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 100,000.

#### Related Topics

- [Standard options for all servers](#)

## 16.4 Job servers

This section provides the command-line options that are specific to Adaptive Job Servers.

The default path to the server on Windows is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\JobServer.exe`.

The default path to the server on Unix is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/boe_jobsd`.

#### Note:

Do not use command-line parameters to set Adaptive Job Server properties. Instead, set the parameters in the CMC as server properties.

Option	Valid Arguments	Behavior
<code>-dir</code>	<i>absolute path</i>	Specify the data directory for the Job Server.

Option	Valid Arguments	Behavior
<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-upperbound</i>	Specify the range of ports that child processes should use in a firewall environment. For example, 6800-6805 limits child processes to six ports. <b>Note:</b> For this option to take effect, you must also specify the <code>-requestPort</code> setting.
<code>-report_ProcessExtPath</code>	<i>absolutepath</i>	Specify the default directory for processing extensions. For details, see the <i>Information Platform Services Administrator Guide</i> .

**Related Topics**

- [Standard options for all servers](#)

**16.5 Adaptive Processing Server**

The Adaptive Processing Server uses parameters defined for the SAP Java Virtual Machine (SAP JVM). Refer to SAP JVM documentation for more information.

**16.6 Input and Output File Repository Servers**

This section provides command-line options for the Input and Output File Repository Servers.

The default path to the servers on Windows is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\fileserver.exe`.

The default paths to the program that provides both servers on Unix is `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/boe_filesd`.

**Note:**

Do not use command-line parameters to set Input and Output File Repository Server properties. Instead, set the parameters in the CMC as server properties.

**Related Topics**

- [Standard options for all servers](#)

# Rights appendix

## 17.1 About the rights appendix

This rights appendix lists and describes most rights that can be set on different objects in the Information platform services 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 Information platform services rights model, see the *Setting Rights* chapter in the *Information platform services Administrator's Guide*.

## 17.2 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.
- 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 Information platform services 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 the "Setting Rights" chapter of the <i>Information platform services Administrator's Guide</i> .
"Define server groups to process jobs"	<p>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.</p> <p>To specify a server group, you also require the "Edit objects" right on the object.</p>
"Delete objects"	Lets you delete objects and their instances.
"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><b>Note:</b> 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.

Right	Description
"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"> <li>• This right on the user or group.</li> <li>• The "Schedule the document to run" right on the object.</li> </ul>
"Schedule to destinations"	<p>Lets you do the following:</p> <ul style="list-style-type: none"> <li>• Schedule objects to destinations other than the default Enterprise location.</li> <li>• Modify the default destinations specified for scheduling.</li> </ul> <p>To schedule the object to destinations, you also require the following rights:</p> <ul style="list-style-type: none"> <li>• The "Schedule the document to run" right on the object that you want to schedule.</li> <li>• The "Add objects to the folder" right on the recipient inbox (if you want to schedule to an inbox destination).</li> <li>• 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).</li> </ul>
"View document instances"	Lets you view object instances. This right is a basic right that is required for all tasks that you perform on object instances.
"Delete instances"	Lets you delete object instances only. If you have the "Delete objects" right, you do not require this right to delete instances.
"Pause and resume document instances"	Lets you pause or resume object instances that are running.
"Reschedule instances"	Lets you reschedule object instances.

### Related Topics

- [Owner rights](#)
- [Choosing between Modify the rights users have to objects options](#)

## 17.3 Rights for specific object types

### 17.3.1 Folder rights

To make rights administration easier, it is recommended that you set rights on folders so that their contents inherit security settings. Folder rights include the following:

- General rights that apply to the folder object.
- Type-specific rights that are intended for the folder's contents (such as the **Print the report's data** right on Crystal reports).

### 17.3.2 Categories

The rights in this section are general rights that have a specific meaning in the context of public and personal categories.

**Note:**

Objects in categories do not inherit rights that are set on the categories.

Right	Description
"Add objects to the folder"	Lets you create new categories within categories. This right is not needed to add objects to a category.
"Edit objects"	<p>Lets you do the following:</p> <ul style="list-style-type: none"> <li>• Modify category properties.</li> <li>• Move the category into another category as a sub-category.</li> <li>• Add objects to the category.</li> <li>• Remove objects from the category.</li> </ul> <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"> <li>• The "Delete objects" right on the original category.</li> <li>• The "Add objects to the folder" right on the destination category.</li> </ul>
"Delete objects"	Lets you delete the category.

### 17.3.3 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"> <li>• Start and reply to discussion threads.</li> <li>• View notes on a discussion thread.</li> <li>• Modify or delete notes that you posted.</li> </ul>

### 17.3.4 Users and groups

You can set rights on users and groups as you would on other objects in the Information platform services 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"> <li>• Edit properties for the user or group.</li> <li>• Manage group membership.</li> </ul> <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"> <li>• Change the password for your user account. To do this, you also require the "Edit objects" right on your user account.</li> <li>• 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.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• This right does not affect the following user password settings: <ul style="list-style-type: none"> <li>• "Password never expires"</li> <li>• "User must change password at next logon"</li> <li>• "User cannot change password"</li> </ul> </li> <li>• This right does not apply to data source credentials for Business Objects Universes.</li> </ul>
"Subscribe to publications"	Lets you add the user to publications as a recipient.
"Schedule on behalf of other users"	Lets you schedule objects on behalf of the user so that the user becomes the owner of the object instance. To do this, you also require the "Schedule on behalf of other users" right on the object.

### 17.3.5 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](#)

## **17.3.6 Applications**

### **17.3.6.1 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.

### 17.3.6.2 Alerting

The rights in this section apply to the Alerting application only.

Right	Description
""Trigger Alerts""	<p>Lets you trigger alert events.</p> <p>To trigger an alert for a document, you need the following rights:</p> <ul style="list-style-type: none"> <li>• View and Schedule rights on the document</li> <li>• View and Trigger rights on the corresponding event</li> </ul>
""Subscribe to Objects""	<p>Lets you subscribe to an alert event</p> <p>To subscribe to an event, you need the following rights:</p> <ul style="list-style-type: none"> <li>• View right on the corresponding event</li> <li>• Subscribe right on the user's own account</li> </ul> <p>To subscribe to an alert in a document, you need the following rights:</p> <ul style="list-style-type: none"> <li>• View right on the document</li> <li>• View Instance right on the document</li> <li>• View right on the corresponding event</li> <li>• Subscribe right on the user's own account</li> </ul>

# Server properties appendix

## 18.1 About the server properties appendix

This server properties appendix lists and describes properties that can be set for each Information platform services server.

### 18.1.1 Common server properties

The server properties described in this section apply to all server types.

Table 18-1: Request port properties

Property	Description	Default value
<b>Server Name</b>	The name of the server	The name of the node that the server is on, plus the name of the server
<b>ID, CUID</b>	The short ID and cluster unique ID of the server. This property is read-only.	Values are auto-generated.
<b>Node</b>	The name of the node where the server is located and, in brackets, the host name and the account name used to run the node	Specified during installation
<b>Description</b>	The server's description	Name of the server
<b>Command Line Parameters</b>	The command-line parameters for the server	Depends on the type of server

Property	Description	Default value
<b>Request Port</b>	<p>Specifies the port from which the server receives requests. 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. If you are specifying a port for the server, ensure that the port is not already taking by another process.</p> <p><b>Note:</b> If <b>Auto assign</b> is set to TRUE, the server binds to a dynamically allocated port. A random port number is allocated to the server each time the server is restarted.</p>	Blank
<b>Auto assign</b>	<p>Specifies whether the server binds to a dynamically allocated port whenever the server is restarted. To bind the server to a specific port, set <b>Auto Assign</b> to FALSE and specify a valid <b>Request Port</b>.</p>	TRUE

Table 18-2: Auto-start properties

Property	Description	Default value
<b>Automatically start this server when the Server Intelligence Agent starts</b>	<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>	TRUE

Table 18-3: Host identifier properties

Property	Description	Default value
<b>Auto assign</b>	<p>Specifies whether the server binds to a network interface that is automatically assigned. If set to FALSE, the server binds to a specific network interface. If set to TRUE, the server accepts requests on the first available IP address. On multihomed computers, you can specify a particular network interface to bind to by setting this value to FALSE and providing a valid hostname or IP address.</p>	TRUE

Property	Description	Default value
<b>Hostname</b>	The hostname of the network interface that the server binds to. If a hostname is specified, the server accepts requests on all IP addresses associated with the hostname.	Blank
<b>IP Address</b>	The IP address of the network interface that the server binds to. Both IPv4 and IPv6 protocols are supported. If an IP address is specified, the server accepts requests on the IP address only.	Blank

Table 18-4: Configuration template properties

Property	Description	Default value
<b>Use Configuration Template</b>	Specifies whether to use a configuration template	FALSE
<b>Restore System Defaults</b>	Specifies whether to restore the original default settings for this server	FALSE
<b>Set Configuration Template</b>	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 for <b>Use Configuration Template</b> are immediately reconfigured to use the settings of the current service.	FALSE

Table 18-5: TraceLog Service properties

Property	Description	Default value
<b>Log Level</b>	Specifies the minimum severity of messages that you want to be recorded, and determines how much information is recorded in the server log file. Possible log threshold levels are: <ul style="list-style-type: none"> <li>• <b>Unspecified</b></li> <li>• <b>None</b></li> <li>• <b>Low</b></li> <li>• <b>Medium</b></li> <li>• <b>High</b></li> </ul>	<b>Unspecified</b>

**Related Topics**

- [Working with configuration templates](#)
- [Trace log levels](#)

**18.1.2 Core Services properties**

The Core services category includes the following servers:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Web Application Container Server

**Adaptive Job Server properties**

Table 18-6: General properties

Property	Description	Default value
<b>Temporary Directory</b>	<p>Specifies the directory where temporary files are created on when necessary. You may encounter performance issues if this directory does not have adequate disk space. For better performance, ensure that this directory is located on a local disk.</p> <p><b>Note:</b> You must restart the server for changes to take effect.</p>	%Default DataDir%

The Adaptive Job Server can host a number of different services. Each service has the following properties:

Table 18-7: Service properties

Property	Description	Default value
<b>Maximum Concurrent Jobs</b>	<p>Specifies the number of concurrent independent processes (child processes) that the server allows. You can adjust the maximum number of jobs to suit your reporting environment.</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>	5
<b>Maximum Child Requests</b>	Specifies the number of jobs the child will process before restarting.	100

**Adaptive Processing Server properties**

Table 18-8: Adaptive Processing Server general properties

Property	Description	Default value
<b>Service Startup Timeout (seconds)</b>	<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"> <li>The service failed, for example, because a required resource such as a database could not be found, or the service encountered a port conflict.</li> <li>The service could not start within the specified time, for example, because the system is too slow.</li> </ul> <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>	1200

Table 18-9: Client Auditing Proxy Service properties

Property	Description	Default value
No configuration properties		

Table 18-10: Publishing Service properties

Property	Description	Default value
No configuration properties		

Table 18-11: Translation Service properties

Property	Description	Default value
No configuration properties		

Table 18-12: Security Token Service properties

Property	Description	Default value
No configuration properties		

Table 18-13: Monitoring Service properties

Property	Description	Default value
No configuration properties		

Table 18-14: Platform Search Service properties

Property	Description	Default value
No configuration properties		

Table 18-15: Publishing Post Processing Service properties

Property	Description	Default value
No configuration properties		

### Central Management Server properties

**Note:**

When you modify any of these server properties, you must restart the server for the changes to take effect.

Table 18-16: Central Management Service properties

Property	Description	Default value
<b>Name Server Port</b>	Specifies the port on which the CMS listens to initial name service requests.	6400
<b>System Database Connections Re-requested</b>	Specifies the number of CMS system database connections that the CMS attempts to establish. If the server cannot establish all of the requested database connection, the CMS continues to function but at a reduced performance, since fewer concurrent requests can be served simultaneously. The CMS will attempt to establish additional connections, until the requested number of connection is established.  The CMS's <b>Established System Database Connections</b> metric shows the current number of established connections.	14
<b>Auto Reconnect to System Database</b>	Specifies whether the CMS automatically attempts to reestablish a connection to the CMS database in the event of a service disruption. If this value is set to FALSE, you are able to check the integrity of the CMS database before resuming operations; you must restart the CMS to reestablish the database connection.	TRUE

Table 18-17: Single Sign-on Service properties

Property	Description	Default value
<b>Single Sign-On Expiry (seconds)</b>	Specifies the time, in seconds, that an SSO connection to a datasource is valid before expiring. This applies to Windows AD users running reports that are configured for Windows AD SSO to the datasource.	86400

**Input File Repository Server properties**

Property	Description	Default value
<b>Maximum Retries for File Access</b>	Specifies the number of times the server tries to access a file.	1

Property	Description	Default value
<b>Maximum Idle Time (minutes)</b>	Specifies the length of time that the server waits before it closes inactive connections. Setting a value that is too low can cause a user's request to be closed prematurely. Setting a value that is too high can cause excessive consumption of system resources such as processing time and disk space.	10
<b>Temporary Directory</b>	Specifies the directory where temporary files are created when necessary. <b>Note:</b> You may encounter performance issues if this directory does not have adequate disk space. For better performance, put the <b>Temporary Directory</b> on the same file system as the <b>File Store Directory</b> .	%DefaultInputFRSDir/temp%
<b>File Store Directory</b>	Specifies the directory where file repository objects are stored. <b>Note:</b> You may encounter performance issues if this directory does not have adequate disk space.	%DefaultInputFRSDir/%

### Output File Repository Server properties

Table 18-19: Output Filestore Service properties

Property	Description	Default value
<b>Maximum Retries for File Access</b>	Specifies the number of times the server tries to access a file.	1
<b>Maximum Idle Time (minutes)</b>	Specifies the length of time that the server waits before it closes inactive connections. Setting a value that is too low can cause a user's request to be closed prematurely. Setting a value that is too high can cause excessive consumption of system resources such as processing time and disk space.	10
<b>Temporary Directory</b>	Specifies the directory where temporary files are created when necessary. <b>Note:</b> You may encounter performance issues if this directory does not have adequate disk space. For better performance, put the temporary directory on the same file system as the file store directory.	%DefaultOutputFRSDir/temp%

Property	Description	Default value
<b>File Store Directory</b>	<p>Specifies the directory where file repository objects are stored.</p> <p><b>Note:</b> You may encounter performance issues if this directory does not have adequate disk space.</p>	%DefaultOutputFRS Dir/%

**Web Application Container Server properties**

Table 18-20: General properties

Property	Description	Default value
<b>Service Startup Timeout (seconds)</b>	<p>How long the WACS will wait for its hosted services to start before it times out. If the timeout passes, the WACS will not provide services that haven't started yet. On a slower machine, you can consider specifying a larger value.</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>	1200

Table 18-21: BOE Web Application Service properties

Property Type	Description	Default value
<b>Authentication Type</b>	<p>The authentication type that is used to authenticate users logging on to Information platform services BI launch pad.</p> <p>Accepted values are:</p> <ul style="list-style-type: none"> <li>• <b>AD Kerberos</b></li> <li>• <b>AD Kerberos SSO</b></li> <li>• <b>Enterprise</b></li> <li>• <b>LDAP</b></li> </ul>	Enterprise

Property Type	Description	Default value
<b>Default AD Domain</b>	The default Active Directory domain is used so that users do not have to supply a domain when they log in. For example, if the default domain is set to "mydomain" and a user logs on with the username "user", the Active Directory logon authority tries to authenticate "user@my-domain.com".	By default, this value is blank.
<b>Service Principal Name</b>	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	By default, this value is blank.
<b>Keytab File</b>	The full path to a keytab file. A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	By default, this value is blank.

Table 18-22: Web Services SDK and QaaWS Service properties

Property	Description	Default value
<b>Enable Kerberos Active Directory Single Sign On</b>	Whether to enable Kerberos AD Single Sign-on for Web Services SDK and QaaWS.	FALSE
<b>Default AD Domain</b>	The default Active Directory domain is used so that users do not have to supply a domain when they log in.	By default, this value is blank.
<b>Service Principal Name</b>	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	By default, this value is blank.

Property	Description	Default value
<b>Keytab File</b>	The full path to a keytab file. A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	By default, this value is blank.

Table 18-23: HTTP configuration properties

Property	Description	Default value
<b>Bind to All IP Addresses</b>	Whether to bind to all network interfaces or not. If your server has more than one NIC, and you want to bind to a specific network interface, uncheck this property.	TRUE
<b>Bind to Hostname or IP Address</b>	Specifies the network interface (IP address or host name) on which HTTP service is provided. You can specify a value only if you clear the <b>Bind to All IP Addresses</b> check box.	localhost
<b>HTTP Port</b>	The port on which HTTP service is provided.	6405 The range of allowed values is 1 to 65535.
<b>Maximum HTTP Header Size</b>	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

Table 18-24: HTTP through proxy configuration properties

Property	Description	Default value
<b>Enable HTTP through Proxy</b>	Whether to enable the HTTP through Proxy connector on the WACS. This is typically checked in deployments with a reverse proxy.	FALSE

Property	Description	Default value
<b>Bind to All IP Addresses</b>	Whether to bind the HTTP through proxy port to all network interfaces or not.	TRUE
<b>Bind to Hostname or IP Address</b>	Specifies the network interface (IP address or host name) on which HTTP through Proxy service is provided. You can specify a value only if you clear the <b>Bind to All IP Addresses</b> check box.	localhost
<b>HTTP Port</b>	The port on which HTTP service in a reverse proxy deployment is provided. You can specify a value only if you select <b>Enable HTTP through Proxy</b> .	6406 The range of allowed values is 1 to 65535.
<b>Proxy Hostname</b>	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can specify a value only if you select <b>Enable HTTP through Proxy</b> .	By default, this value is blank.
<b>Proxy Port</b>	The port of your forward or reverse proxy server. You can specify a value only if you select <b>Enable HTTP through Proxy</b> .	0 The range of allowed values is 1 to 65535.
<b>Maximum HTTP Header Size</b>	The maximum allowed size, in bytes, of the request and response HTTP header. You can specify a value only if you select <b>Enable HTTP through Proxy</b> .	32768

Table 18-25: HTTPS configuration properties

Property	Description	Default value
<b>Enable HTTPS</b>	Whether to enable HTTPS/SSL communication.	FALSE

Property	Description	Default value
<b>Bind to Hostname or IP Address</b>	Specifies the network interface (IP address or host name) on which HTTPS service is provided. You can specify a value only if you select <b>Enable HTTPS</b> .	localhost
<b>HTTPS Port</b>	The port on which HTTPS service is provided. You can specify a value only if you select <b>Enable HTTPS</b> .	443 The range of allowed values is 1 to 65535.
<b>Proxy Hostname</b>	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can specify a value only if you select <b>Enable HTTPS</b> .	By default, this value is blank.
<b>Proxy Port</b>	The port of your forward or reverse proxy server. You can specify a value only if you select <b>Enable HTTPS</b> .	0 The range of allowed values is 1 to 65535.
<b>Protocol</b>	The encryption protocol to use. You can specify a value only if you select <b>Enable HTTPS</b> .	TLS The allowed values are TLS or SSL.
<b>Certificate Store Type</b>	The type of certificate store that contains your certificates and private keys. In most cases, this will be PCKS12. You can specify a value only if you select <b>Enable HTTPS</b> .	PKCS12 The allowed values are PKCS12 or JKS.
<b>Certificate Store File Location</b>	The full path to the certificate file. You can specify a value only if you select <b>Enable HTTPS</b> .	By default, this value is blank.

Property	Description	Default value
<b>Private Key Access Password</b>	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 specify a value only if you select <b>Enable HTTPS</b> .	By default, this value is blank.
<b>Certificate Alias</b>	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 specify a value only if you select <b>Enable HTTPS</b> .	By default, this value is blank.
<b>Enable Client Authentication</b>	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 select <b>Enable HTTPS</b> .	FALSE
<b>Certificate Trust List File Location</b>	The full path to the certificate trust list file. You can specify a value only if you select <b>Enable HTTPS</b> and <b>Enable Client Authentication</b> .	By default, this value is blank.
<b>Certificate Trust List Private Key Access Password</b>	The password that protects access to the private keys in the Certificate Trust List file. You can specify a value only if you select <b>Enable HTTPS</b> and <b>Enable Client Authentication</b> .	By default, this value is blank.

Property	Description	Default value
<b>Maximum HTTP Header Size</b>	The maximum allowed size, in bytes, of the request and response HTTP header. You can specify a value only if you select <b>Enable HTTPS</b> .	32768

Table 18-26: Concurrency settings (per connector)

Property	Description	Default value
<b>Maximum Concurrent Requests</b>	The number of concurrent HTTP or HTTPS requests that each connector (HTTP, HTTP through Proxy, or HTTPS) can process simultaneously.	150 The range of allowed values is 1 to 9999.

Table 18-27: Active directory configuration settings

Property	Description	Default value
<b>Krb5.ini File Location</b>	The full path to a <code>krb5.ini</code> file that stores Kerberos configuration properties.	By default, this value is blank.
<b>bscLogin.conf File Location</b>	The full path to a <code>bscLogin.conf</code> file.	By default, this value is blank.



# Server metrics

## 19.1 About the Server Metrics Appendix

In this appendix unless otherwise stated, the term server refers to an SAP BusinessObjects server, and not to the machine that Information platform services is installed or running on.

Server metrics are not available on servers that are not running.

### Related Topics

- [Analyzing server metrics](#)

### 19.1.1 Common Server Metrics

The following metrics describe the machine that the specified server is running on.

Table 19-1: Machine-specific metrics

Metric	Description
Machine Name	The host name of the machine that the server is running on.
Operating System	The operating system of the machine that the server is running on.
CPU Type	The type of Central Processing Units of the machine that the server is running on. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).

<b>Metric</b>	<b>Description</b>
<b>CPUs</b>	The number of CPUs that are available to the server. On multi-core hardware, this metric may report the number of logical CPUs, and not the number of physical processors. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
<b>RAM (MB)</b>	The amount of memory in megabytes that is available on the machine that the server is running on. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
<b>Local Time</b>	The local time.
<b>Disk Size (GB)</b>	The size of the disk that Information platform services is installed on, in gigabytes. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
<b>Used Disk Space (GB)</b>	The amount of used space on the disk, in gigabytes, that Information platform services is installed on. This includes disk space that is used by other programs on the machine, and not just space used by Information platform services. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).

The following metrics describe the specified SAP BusinessObjects server.

Table 19-2: Server-specific metrics

<b>Metric</b>	<b>Description</b>
<b>Name Server</b>	The name and port number of the CMS server that this server publishes its address to.
<b>Registered Name</b>	The internal name of the server. This is not the name that appears on the "Servers" screen of the CMC.
<b>Version</b>	The version of the server.
<b>Start Time</b>	The time that the server was most recently started.
<b>PID</b>	The unique Process ID number for the server. The operating system of the machine that the server is running on generates the PID. The PID can be used to identify the specific server.

Metric	Description
<b>Host Name</b>	A comma-separated list of host names that are currently being used by the server.
<b>Host IP Address</b>	A comma-separated list of IP Addresses that the server listens for requests on.
<b>Request Port</b>	The port from which the server receives requests from other servers. If the server is listening to requests on more than one IP Address, the request port for the server will always be the same. If any other process uses this request port, the server will not start. Ensure that other processes do not use this port.
<b>Busy Server Threads</b>	The number of server threads that are currently servicing a request. If this number is the same as the maximum thread pool size of the server, it indicates that the system can't process additional requests in parallel and that new requests may have to wait for busy threads to become available.

Table 19-3: Auditing Metrics

Metric	Description
<b>Current Number of Auditing Events in the Queue</b>	<p>The number of auditing events that an Auditee has recorded, but which have not yet been retrieved by the CMS Auditor. If this number increases without bound, it could indicate that Auditing is not configured correctly or that the system is heavily loaded and generating audit events faster than the Auditor can retrieve them.</p> <p><b>Note:</b> When stopping a server, first disable it and wait for this metric to reach "0". Otherwise you may have auditing events that remain in the queue and do not reach the Auditing Data Store until the server is restarted and the CMS polls for them.</p>

Table 19-4: Logging Service Metrics

Metric	Description
<b>Logging Directory</b>	Log files for the server are available in this location.

## 19.1.2 Central Management Server metrics

The following table describes the server metrics that appear on the "Metrics" screen in the Central Management Server (CMS).

Metric	Description
<b>Connection to Auditing Database is Established</b>	Indicates whether the CMS has a healthy connection to the auditing database. A value of "1" indicates that there is a connection. A value of "0" indicates that there is no connection to the auditing database. If the CMS is an auditor, this value should be "1". If it is "0", investigate why a connection to the Auditing database cannot be established.
<b>CMS Auditor</b>	Indicates if the Central Manager Server (CMS) is acting as an auditor. A value of "1" indicates that the CMS is acting as an auditor. A value of "0" indicates that the CMS is not acting as an auditor.
<b>Auditing Database Connection Name</b>	The name of the auditing database connection. This is not necessarily the name of the auditing database itself. If this metric is empty, it indicates that a connection to the auditing database cannot be established.
<b>Auditing Database User Name</b>	The name of the user account used to connect to the auditing database.
<b>Auditing Database Last Updated On</b>	The most recent date and time that the CMS successfully started to retrieve events from an auditee. If the CMS is an auditor, this metric must show a time that is close to the time that the "Metrics" screen is loaded. If this value is more than two hours prior to the time that the screen is loaded, it may indicate that auditing is not working properly.

Metric	Description
<b>Auditing Thread Last Polling Cycle Duration (seconds)</b>	<p>The duration of the last polling cycle in seconds. This indicates the maximum delay for event data to reach the auditing database during the previous polling cycle.</p> <ul style="list-style-type: none"> <li>• A value of less than 20 minutes indicates a healthy system.</li> <li>• A value between 20 minutes and 2 hours indicates a busy system.</li> <li>• A value of greater than 2 hours indicates a very busy system. If this state persists and you consider the delay too long, it is recommended that you either update your deployment to all the auditing database to receive data at a higher rate or decrease the number of auditing events that your system tracks.</li> </ul>
<b>Auditing Thread Utilization</b>	<p>The percentage of the polling cycle the auditor CMS spends collecting data from auditees. The remainder is time spent resting between polls.</p> <p>If this value reaches 100%, the auditor is still collecting data from the auditees when the next poll is due to begin. This may cause delays in the events reaching the auditing database. If the Thread Utilization frequently reaches 100%, and remains at this rate for several days, it is recommended you either update your deployment to allow the auditing database to receive data at a higher rate, or decrease the number of auditing events that your system tracks.</p>
<b>Clustered CMS Servers</b>	A semicolon-separated list of the host names and port numbers of the running Central Management Servers in the cluster.
<b>Number of Sessions Established by Concurrent Users</b>	The total number of sessions for users with concurrent licensing.
<b>Number of Sessions Established by Named Users</b>	The total number of sessions for users with named licensing.
<b>Peak Number of User Sessions Since Startup</b>	The peak number of concurrent user sessions that the CMS has handled since it was started.
<b>Number of Sessions Established by Servers</b>	The number of concurrent sessions that Information platform services servers have created with the CMS. If this number is greater than 250, create an additional CMS.

Metric	Description
<b>Number of Sessions Established by All Users</b>	The number of concurrent user sessions that are being handled by the CMS at the time that the "Metrics" screen loads. The larger this number is, the larger the number of users that are using the system is. If this number is greater than 250, create an additional CMS.
<b>Failed Jobs</b>	The total number of failed jobs on the CMS since the server started.
<b>Pending Jobs</b>	The current number of jobs that are scheduled, but not ready, to run because the scheduled time or event has not arrived.
<b>Running Jobs</b>	The current number of jobs that are running.
<b>Completed Jobs</b>	The total number of completed jobs on the CMS since the server started.
<b>Waiting Jobs</b>	The current number of waiting jobs on the CMS. This includes jobs that are scheduled and waiting for free resources.
<b>Concurrent User Licenses</b>	The number of Concurrent User licenses as indicated by the key code.
<b>Named User Licenses</b>	The number of Named User licenses as indicated by the key code
<b>Build Date</b>	The build date of the CMS.
<b>System Database Connection Name</b>	The name of the CMS system database connection. This is not necessarily the name of the CMS system database itself.
<b>System Database Server Name</b>	The name of the server where the CMS system database is running. This is not necessarily the name of the CMS system database itself.
<b>System Database User Name</b>	The name of the user account used to connect to the CMS system database.
<b>Data Source Name</b>	The name of the CMS system database connection.
<b>Build Number</b>	The build number of the CMS. This number can be used to identify the version of Information platform services that you have installed.
<b>Product Version</b>	The product version of the CMS.
<b>Resource Version</b>	The resource version of the CMS.

Metric	Description
<b>Average Commit Response Time Since Startup (msec)</b>	The average length of time in milliseconds that it took the CMS to perform commit operations since the server was started. A response time greater than 1000 milliseconds may indicate a need to tune the CMS or the CMS system database.
<b>Average Query Response Time Since Startup (msec)</b>	The average length of time in milliseconds that it took the CMS to perform query operations since the server was started. A response time greater than 1000 milliseconds may indicate a need to tune the CMS or the CMS system database.
<b>Longest Commit Response Time Since Startup (msec)</b>	The longest length of time in milliseconds that it took the CMS to perform commit operations since the server was started. A response time greater than 10000 milliseconds may indicate a need to tune the CMS or the CMS system database.
<b>Longest Query Response Time Since Startup (msec)</b>	The longest length of time in milliseconds that it took the CMS to perform query operations since the server was started. A response time greater than 10000 milliseconds may indicate a need to tune the CMS or the CMS system database.
<b>Number of Commits Since Startup</b>	The number of commits to the CMS system database since the server was started.
<b>Number of Queries Since Startup</b>	The total number of database queries since the server was started. A large number may indicate a more active or heavily loaded system.
<b>Number of User Logons Since Startup</b>	The number of user logons since the server was started. A large number may indicate a more active or heavily loaded system.
<b>Established System Database Connections</b>	The number of connections to the CMS system database that the CMS was able to establish. If a database connection is lost, the CMS attempts to restore the connection. If the number of established database connections is consistently lower than the number of system database connections specified by the <b>System Database Connections Requested</b> property ("Central Management Service" area of the "Properties" screen), the CMS may be unable to acquire additional connections and may not function optimally. A potential solution is to configure the database server to allow more database connections for the CMS.

Metric	Description
<b>Currently Used System Database Connections</b>	The number of connections to the CMS system database that the CMS is currently using. The number of connections that are being currently used may be smaller than or equal to the number of established system database connections. If the number of established connections and the number of used connections are identical for some time, this may indicate a bottleneck. Increasing the value for the <b>System Database Connections Requested</b> property on the "Properties" screen may improve the performance of the CMS. Tuning the CMS system database may also improve performance.
<b>Pending System Database Requests</b>	The number of requests for the CMS system database that are waiting for an available connection. If this number is high, consider increasing the value for the <b>System Database Connections Requested</b> property. Tuning the CMS system database may also improve performance.
<b>Number of Objects in CMS System Cache</b>	The total number of objects that are currently in the CMS system cache.
<b>Number of Objects in CMS System DB</b>	The total number of objects that are currently in the CMS system database.
<b>Existing Concurrent User Accounts</b>	The total number of existing users with concurrent licensing in the cluster.
<b>Existing Named User Accounts</b>	The total number of existing users with named licensing in the cluster.

### 19.1.3 File Repository Server Metrics

The following table describes the server metrics that appear on the "Metrics" screen for Input and Output File Repository Servers.

Table 19-6: Filestore Service Metrics

<b>Metric</b>	<b>Description</b>
<b>Active Files</b>	The number of files in the File Repository Server that are currently being accessed.
<b>Data Written (MB)</b>	The total number of megabytes written to files on the server.
<b>Data Sent (MB)</b>	The total number of megabytes read from files on the server.
<b>List of Active Files</b>	A table that displays the files in the File Repository Server that are currently being accessed.
<b>Active Connections</b>	The total number of active connections from clients and to other servers.
<b>Available Disk Space in Root Directory (GB)</b>	The total amount of available space on the disk containing the server's executable file, in gigabytes.
<b>Free Disk Space in Root Directory (GB)</b>	The total amount of free space on the disk containing the server's executable file, in gigabytes.
<b>Total Disk Space in Root Directory (GB)</b>	The total disk space on the disk containing the server's executable file, in gigabytes.
<b>Available Disk Space in Root Directory (%)</b>	The amount of available disk space, in percentage, on the disk containing the server's executable file.

### 19.1.4 Adaptive Processing Server metrics

The following table describes the server metrics that appear on the "Metrics" page for Adaptive Processing Servers.

Table 19-7: Adaptive Processing Server metrics

<b>Metric</b>	<b>Description</b>
<b>Threads in Transport Layer</b>	The total number of threads in all thread pools of the transport layer.
<b>Transport Layer Thread Pool Size</b>	The total number of shared transport layer threads. These threads can be used by any of the hosted services on the Adaptive Processing Server.

Metric	Description
<b>Available Processors</b>	The number of processors that are available to the Java Virtual Machine (JVM) on which the server is running.
<b>Maximum Memory (MB)</b>	The maximum amount of memory, in megabytes, that the Java virtual machine will attempt to use.
<b>Free Memory (MB)</b>	The amount of memory, in megabytes, that is available to the JVM for allocating new objects.
<b>Total Memory (MB)</b>	The total amount of memory, in megabytes, in the Java virtual machine. This value may vary over time, depending on the host environment.
<b>CPU Usage Percentage (last 5 minutes)</b>	The percentage of total CPU time used by the server during the previous five minutes. For example, if a single thread fully utilizes one CPU of a four-CPU system, the utilization is 25%. All processors allocated to the JVM are considered. A value of greater than 80% may indicate a CPU bottleneck.
<b>CPU Usage Percentage (last 15 minutes)</b>	The percentage of total CPU time used by the server during the previous 15 minutes. For example, if a single thread fully utilizes one CPU of a four-CPU system, the utilization is 25%. All processors allocated to the JVM are considered. A value of greater than 70% may indicate a bottleneck.
<b>Percentage of stopped system during GC (last 5 minutes)</b>	<p>Percentages of stopped system while Garbage Collections (GC) were running during the last five minutes. In this state all APS services are prevented from executing while the virtual machine performs a critical stage of garbage collection that requires exclusive access.</p> <p>Generally, a low single-digit value should be the normal behavior, even under load. A double-digit value over time might indicate an issue of low throughput and needs to be investigated.</p>

Metric	Description
<b>Percentage of stopped system during GC (last 15 minutes)</b>	<p>Percentages of stopped system while Garbage Collections (GC) were running during the last 15 minutes. In this state all application code running on top of the Java virtual machine is prevented from executing while the virtual machine performs a critical stage of garbage collection that requires exclusive access.</p> <p>Generally, a low single-digit value should be the normal behavior, even under load. A double-digit value over time might indicate an issue of low throughput and needs to be investigated.</p>
<b>Number of page faults during GC (last 5 minutes)</b>	The number of page faults that have occurred while Garbage Collections were running during the previous five minutes. Any value greater than 0 indicates a system under heavy load and low memory conditions.
<b>Number of page faults during GC (last 15 minutes)</b>	The number of page faults that have occurred while Garbage Collections were running during the last 15 minutes. Any value greater than 0 indicates a system under heavy load and low memory conditions.
<b>Number of Full GCs</b>	The number of full Garbage Collections since the server has started. A rapid increase in this value may indicate a system under low memory conditions.
<b>JVM Lock Contention Count</b>	The number of synchronized objects that have threads that are waiting for access. Any value consistently greater than 0 may indicate threads that will not run again. Initiate a Thread Dump to obtain more information about the cause of the problem.
<b>JVM Debug Info</b>	Debugging information about the SAP Java Virtual Machine, including the state, port, and attached client, if available.
<b>JVM Version Info</b>	Version information about the SAP Java Virtual Machine.
<b>JVM Deadlocked Threads Counter</b>	The number of threads that are deadlocked. Any value greater than 0 indicates threads that will not run again. Initiate a Thread Dump to obtain more information about the cause of the problem.
<b>JVM Trace Flags</b>	The trace flags that are currently turned on for the JVM. This indicates the level of tracing of the JVM.
<b>Services</b>	A comma-separated list of the services that the server hosts.

Table 19-8: DSL Bridge Service metrics

Metric	Description
<b>DSLServiceMetrics.queryCount</b>	The number of data requests that are open between clients and the service
<b>DSLServiceMetrics.activeConnectionCount</b>	The number of connections that are currently open between clients and the service.
<b>DSLServiceMetrics.activeSessionCount</b>	The number of sessions that are currently open between clients and the service.
<b>DSLServiceMetrics.activeOLAPConnectionCount</b>	The number of connections that are current open between OLAP clients and the service.

Table 19-9: Client Auditing Proxy Service metrics

Metric	Description
<b>Number of Audit Events Received Since Server Startup</b>	The number of client auditing events that the service has received since it was started. This metric can be used to verify that client auditing has been configured correctly. Values greater than "0" indicate that auditing events from clients are being successfully routed through this Client Auditing Service.

Table 19-10: Platform Search Service metrics

Metric	Description
<b>Number of Successful Extraction Attempts since the Service Start</b>	The number of successful attempts for extracting documents since the Platform Search Service was started.
<b>Last Index Update Timestamp</b>	The date and time when the last index update happened
<b>Last Content Store Generation Timestamp</b>	The date and time when the last content store was generated.
<b>Number of failed extraction attempts since the service start</b>	The number of failed attempts for extracting documents since the Platform Search Service was started.
<b>Service Available</b>	TRUE if the service is available. Otherwise FALSE.
<b>Indexing Running</b>	TRUE if the indexing is running. Otherwise FALSE.

<b>Metric</b>	<b>Description</b>
<b>Number of Documents Indexed</b>	The displays the number of documents that were indexed since the service was started.

Table 19-11: Multi Dimensional Analysis Service metrics

<b>Metric</b>	<b>Description</b>
<b>Session Count</b>	The current number of connections from MDAS clients to the server.
<b>Cube Count</b>	The number of data sources that are being used to supply data to the connections that have not timed out.
<b>Query Count</b>	The number of data requests that are open between MDS clients and the server.

Table 19-12: Data Federation Service metrics

<b>Metric</b>	<b>Description</b>
<b>Number of Running Queries</b>	The total number of running queries (consuming memory or not).
<b>Number of Connections</b>	The total number of user connections to data federation query engine.
<b>Total Bytes Transferred from Data Sources</b>	The amount of data read from the data sources (in bytes).
<b>Total Records Transferred from Data Sources</b>	The total number of rows read from the data sources.
<b>Total Bytes Produced by Query Execution</b>	The amount of data produced as output of queries (in bytes).
<b>Total Records Produced by Query Execution</b>	The total number of rows produced as output of queries.
<b>Number of Queries Consuming Memory</b>	The total number of running queries consuming memory.
<b>Total Bytes of Memory Used by Query Execution</b>	The amount of memory currently used by the running queries (in bytes).
<b>Total Bytes of Disk Used by Query Execution</b>	The amount of disk currently used by the running queries (in bytes).

<b>Metric</b>	<b>Description</b>
<b>Number of Queries Using Disk</b>	The total number of running queries using disk.
<b>Number of Queries Waiting for Resources</b>	The total number of running queries currently waiting for execution.
<b>Number of Active Threads</b>	The total number of active threads used for used for execution of requests.
<b>Total Bytes of Memory Used by Metadata Cache</b>	The amount of memory used for caching metadata, statistics and connectors configuration (in bytes).
<b>Number of Failed Queries</b>	The total number of failed queries (exception raised).
<b>Number of Queries in Query Analyze Step</b>	The total number of running queries currently in analyze step.
<b>Number of Queries in Query Optimization Step</b>	The total number of running queries currently in optimization step.
<b>Number of Queries in Query Execution Step</b>	The total number of running queries currently in execution step.
<b>Number of Loaded Connectors</b>	The total number of connectors loaded in the service.
<b>Number of Active Connections to Loaded Connectors</b>	The total number of active connections to connectors loaded in the service.
<b>Data Federation Service is available</b>	TRUE if the service is available (FALSE if the service is unavailable)

Table 19-13: Connectivity Service metrics

Metric	Description
<b>Data Sources</b>	<p>Lists in a table the data sources activated on the "Properties" page. Displays the following information for each network layer and database pair:</p> <ul style="list-style-type: none"> <li>• Status ("Loaded" or "Failed"): The current status of the driver</li> <li>• Available connections: The number of pool connections that can be used</li> <li>• Jobs (CORBA): The number of jobs that are being processed (in a 2-tier deployment)</li> <li>• Jobs (HTTP): The number of jobs that are being processed (in a web-tier deployment)</li> </ul> <p>For more information about connection pools, see the <i>Data Access Guide</i>.</p>

### 19.1.5 Web Application Container Server metrics

The following table describes the server metrics that appear on the "Metrics" page for Web Application Container Servers.

**Note:**

The Adaptive Processing Server metrics also apply to Web Application Container Servers.

Metric	Description
<b>List of Running WACS Connectors</b>	A list of all running connectors on the server. If you do not see all of the connectors (HTTP, HTTPS and HTTP through proxy), it indicates either that the connector is not enabled or that it failed during startup
<b>WACS Connector(s) Failed at Startup</b>	Whether there are any failed connectors. If true, at least one connector failed to start. If false, all connectors are running. Do not run a server when one or more connectors has failed to start; you must troubleshoot the server to ensure that all connectors start properly.

**Related Topics**

- [Adaptive Processing Server metrics](#)

**19.1.6 Adaptive Job Server metrics**

Table 19-16: Job Server metrics

<b>Metric</b>	<b>Description</b>
<b>Received Job Requests</b>	The number of jobs that were supposed to have run on the server.
<b>Concurrent Jobs</b>	The number of jobs that are currently running on the server. If this number is high, the server is busy.
<b>Peak Jobs</b>	The maximum number of concurrent jobs that have run at the same time on the server. This number never goes down until the server is restarted.
<b>Failed Job Creations</b>	The number of jobs that failed on the server.
<b>Temporary Directory</b>	The directory where temporary files are created. This can be specified on the "Properties" screen for the server.  You may encounter issues if this directory does not have adequate disk space.
<b>File System Destination Default Settings Valid</b>	TRUE if the server is able to send documents to the File System Destination that is specified on the "Destination" screen for the server. (If not, it is set to FALSE.)
<b>FTP Destination Default Settings Valid</b>	TRUE if the server is able to send documents to the FTP Server Destination that is specified on the "Destination" screen for the server. (If not, it is set to FALSE.)
<b>Inbox Destination Default Settings Valid</b>	TRUE if the server is able to send objects to the Inbox Destination that is specified on the "Destination" screen for the server. (If not, it is set to FALSE.)
<b>Email Destination Default Settings Valid</b>	TRUE if the server is able to send objects to the Email Destination that is specified on the "Destination" screen for the server. (If not, it is set to FALSE.)

<b>Metric</b>	<b>Description</b>
<b>Scheduling Services</b>	A table that displays the scheduling services that are running on the server.
<b>Children</b>	A table that displays the child processes that are running on the server.
<b>JSDPC?m_name=CrystalEnterprise.StreamWork</b>	
<b>JSDPC?m_name=CrystalEnterprise.StreamWorkEx</b>	

The following table describes the metrics for each Scheduling Service that is running on the server.

*Table 19-17: Scheduling Service metrics*

<b>Metric</b>	<b>Description</b>
<b>Scheduling Service</b>	The name of the service.
<b>Received Job Requests</b>	The number of jobs that were supposed to have run on the service.
<b>Concurrent Jobs</b>	The number of concurrent jobs that are currently running on the service. If this number is high, the service is busy.
<b>Peak Jobs</b>	The maximum number of concurrent jobs that have run at the same time on the service.
<b>Maximum Concurrent Jobs Allowed</b>	The number of concurrent independent processes (child processes) that the service allows. This can be specified on the "Properties" screen for the server.
<b>Failed Job Creations</b>	The number of jobs that failed on the service.

The following table describes the metrics for each child process that is running on the server.

*Table 19-18: Child metrics*

<b>Metric</b>	<b>Description</b>
<b>Scheduling Service</b>	The name of the scheduling service that the child process is using.
<b>PID</b>	The child process's identifier.

<b>Metric</b>	<b>Description</b>
<b>Received Job Requests</b>	The number of jobs that were supposed to have run on the child process.
<b>Concurrent Jobs</b>	The number of concurrent jobs that are currently running on the child process. Normally this number must be 1.
<b>Peak Jobs</b>	The maximum number of concurrent jobs that have run at the same time on the child process.
<b>Maximum Jobs Allowed</b>	The number of concurrent jobs that the child process allows.
<b>Comm. Failures</b>	The number of communication failures with the parent Adaptive Job Server that have occurred. If this number is large, the child process will restart.
<b>Initializing</b>	1 if the child process is in the process of initializing (If not, it is set to 0.)
<b>Shutting Down</b>	1 if the child process is in the process of shutting down (If not, it is set to 0.)

## Nodes and placeholders

### 20.1 Server and node placeholders

Except for `%SERVER_FRIENDLY_NAME%` and `%SERVER_NAME%`, the following placeholders apply to all servers on the same node.

Placeholder	Description	Default values
<code>%AuditingDatabaseConnection%</code>	The Auditing Database connection used by the CMS.	Specified during installation
<code>%AuditingDatabaseDriver%</code>	The type of database driver that is used to connect to the Auditing database.	Depends on the database used—for example: <ul style="list-style-type: none"> <li>For SQL Server: <code>sqlserverauditdbss</code></li> <li>For MySQL: <code>mysqlauditdbss</code></li> </ul>
<code>%BINDIR%</code>	The folder where Information platform services 64-bit binaries are located.	<ul style="list-style-type: none"> <li>On Windows: <code>&lt;INSTALLEDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/win64_x64</code></li> <li>On Unix: <code>&lt;INSTALLEDIR&gt;/sap_bobj/enterprise_xi40/&lt;platform64&gt;</code></li> </ul>
<code>%BINDIR32%</code>	The folder where Information platform services 32-bit binaries are located.	<ul style="list-style-type: none"> <li>On Windows: <code>&lt;INSTALLEDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/win32_x86</code></li> <li>On Unix: <code>&lt;INSTALLEDIR&gt;/sap_bobj/enterprise_xi40/&lt;platform32&gt;</code></li> </ul>
<code>%CACHESERVER_EXE%</code>	The name of the executable for the Crystal Reports Cache Server.	<ul style="list-style-type: none"> <li>On Windows: <code>crcache.exe</code></li> <li>On Unix: <code>boe_crcached.bin</code></li> </ul>

Placeholder	Description	Default values
<b>%CMS_EXE%</b>	The name of the executable for the Central Management Server.	<ul style="list-style-type: none"> <li>• On Windows: cms.exe</li> <li>• On Unix: boe_cmsd</li> </ul>
<b>%CONNECTIONSERVER32_EXE%</b>	The name of the executable for the 32-bit Connection Server.	<ul style="list-style-type: none"> <li>• On Windows: ConnectionServer32.exe</li> <li>• On Unix: ConnectionServer32</li> </ul>
<b>%CONNECTIONSERVER_DIR%</b>	The root folder of the Connection Server.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/dataAccess/connectionServer</li> <li>• On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/dataAccess/connectionServer</li> </ul>
<b>%CONNECTIONSERVER_EXE%</b>	The name of the executable for the 64-bit Connection Server.	<ul style="list-style-type: none"> <li>• On Windows: ConnectionServer.exe</li> <li>• On Unix: ConnectionServer</li> </ul>
<b>%CR2011_BINDIR%</b>	The directory where Crystal Reports 2011 server binaries are located.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/win32_x86</li> <li>• On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM32&gt;/</li> </ul>
<b>%CR2011_DefaultWorkingDir%</b>	The default working directory for Crystal Reports 2011 servers.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/win32_x86</li> <li>• On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM32&gt;/</li> </ul>

Placeholder	Description	Default values
<b>%CRYSTALRAS_EXE%</b>	The name of the executable for the Report Application Server.	<ul style="list-style-type: none"> <li>On Windows: On Unix, &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM32&gt;/crystalras.exe</li> <li>On Unix: boe_crystalrasd</li> </ul>
<b>%CR_ODBCINI%</b>	The name and path of the .odbc.ini file is located.	<ul style="list-style-type: none"> <li>On Windows: This placeholder is blank.</li> <li>On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/odbc.ini</li> </ul>
<b>%CommonJavaBundlesDir%</b>	<p>The folder where shared OSGI bundles are located.</p> <ul style="list-style-type: none"> <li>On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/java/lib/bundles</li> <li>On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/java/lib/bundles</li> </ul>	<ul style="list-style-type: none"> <li>On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/java/lib/bundles</li> <li>On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/java/lib/bundles</li> </ul>
<b>%CommonJavaLibDir%</b>	The folder where the common Java libraries are located.	<ul style="list-style-type: none"> <li>On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/java/lib</li> <li>On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/java/lib</li> </ul>
<b>%DLLEXT%</b>	The default extension of a .dll or .so file.	<ul style="list-style-type: none"> <li>On Windows: .dll</li> <li>On Unix: .so</li> </ul>
<b>%DLLPATH%</b>	The name of the environment variable on the machine on which Information platform services is installed that specifies the directories where the interpreter will search for executable files.	<ul style="list-style-type: none"> <li>On Windows: Path</li> <li>On Unix: LD_LIBRARY_PATH</li> </ul>

Placeholder	Description	Default values
<b>%DLLPATH32%</b>	On Solaris 32-bit systems, The name of the environment variable on the machine on which Information platform services is installed that specifies the directories where the interpreter will search for executable files.	<ul style="list-style-type: none"> <li>On Windows and Linus: This placeholder is blank.</li> <li>On AIX: <i>LDR_PRELOAD</i></li> <li>On Solaris: <i>LD_PRELOAD_32</i></li> </ul>
<b>%DLLPATH64%</b>	On Solaris 64-bit systems, the name of the environment variable on the machine on which Information platform services is installed that specifies the directories there the interpreter will search for executable files.	<ul style="list-style-type: none"> <li>On AIX: <i>LDR_PRELOAD64</i></li> <li>On Solaris: <i>LD_PRELOAD_64</i></li> <li>Other operating systems: This placeholder is blank.</li> </ul>
<b>%DLLPREFIX%</b>	The default prefix of a .dll or .so file.	<ul style="list-style-type: none"> <li>On Windows: This placeholder is blank.</li> <li>On Unix: lib</li> </ul>
<b>%DLLPRELOAD%</b>	The name of the <i>LD_PRELOAD</i> environment variable for the platform.	<ul style="list-style-type: none"> <li>On Windows: This placeholder is blank.</li> <li>On AIX: <i>LDR_PRELOAD64</i></li> <li>On other Unix: <i>LD_PRELOAD</i></li> </ul>
<b>%DLLPRELOAD32%</b>	The name of the <i>LD_PRELOAD</i> environment variable on 32-bit AIX systems.	<ul style="list-style-type: none"> <li>On AIX: <i>LDR_PRELOAD</i></li> <li>On Solaris: <i>LD_PRELOAD_32</i></li> <li>On Linus, Windows, and other operating systems: This placeholder is blank.</li> </ul>
<b>%DLLPRELOAD64%</b>	The name of the <i>LD_PRELOAD</i> environment variable on 64-bit AIX systems.	<ul style="list-style-type: none"> <li>On AIX, <i>LDR_PRELOAD64</i></li> <li>On Solaris: <i>LD_PRELOAD_64</i></li> <li>On Linus, Windows, and other operating systems: This placeholder is blank.</li> </ul>
<b>%DP%</b>	The path delimiter.	<ul style="list-style-type: none"> <li>On Windows: Semicolon (;)</li> <li>On Unix: Colon (:)</li> </ul>

Placeholder	Description	Default values
<b>%DefaultAuditingDir%</b>	The directory where Auditing temporary files are written. For optimum performance, this location should be on the server's local drive.	<ul style="list-style-type: none"> <li>• <b>On Windows:</b> &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/Auditing</li> <li>• <b>On Unix:</b> &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/data/Auditing/</li> </ul>
<b>%DefaultDataDir%</b>	The temporary directory used by the Job Server.	<ul style="list-style-type: none"> <li>• <b>On Windows:</b> &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/Data</li> <li>• <b>On Unix:</b> &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/data/</li> </ul>
<b>%DefaultInputFRSDir%</b>	The root folder of the Input File Repository Server.	<ul style="list-style-type: none"> <li>• <b>On Windows:</b> &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/FileStore/Input</li> <li>• <b>On Unix:</b> &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/data/frsinput</li> </ul>
<b>%DefaultLoggingDir%</b>	The location where the log files are stored.	<ul style="list-style-type: none"> <li>• <b>On Windows:</b> &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/logging</li> <li>• <b>On Unix:</b> &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/logging</li> </ul>
<b>%DefaultOutputFRSDir%</b>	The root folder of the Output File Repository Server.	<ul style="list-style-type: none"> <li>• <b>On Windows:</b> &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/FileStore/Output</li> <li>• <b>On Unix:</b> &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/data/frsoutput</li> </ul>

Placeholder	Description	Default values
<b>%DefaultWorkingDir%</b>	The working directory for 64-bit servers	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/win64_x64</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM64&gt;</li> </ul>
<b>%DefaultWorkingDir32%</b>	The working directory for 32-bit servers.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/win32_x86</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM32&gt;</li> </ul>
<b>%EVENTSERVER_EXE%</b>	The name of the executable for the Event Server.	<ul style="list-style-type: none"> <li>• On Windows: EventServer.exe</li> <li>• On Unix: boe_eventsd</li> </ul>
<b>%EXEEXT%</b>	The default extension of executable files.	<ul style="list-style-type: none"> <li>• On Windows: .exe</li> <li>• On Unix: This placeholder is unavailable.</li> </ul>
<b>%EXEPATH%</b>	The name of the environment variable on the machine on which Information platform services is installed that specifies the directories there the interpreter will search for executable files.	<ul style="list-style-type: none"> <li>• On Windows: <i>Path</i></li> <li>• On Unix: <i>PATH</i></li> </ul>
<b>%EnterpriseDir%</b>	The location where 64-bit Information platform services is installed.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40</li> </ul>

Placeholder	Description	Default values
<b>%EnterpriseDir32%</b>	The location where 32-bit Information platform services is installed.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40</li> </ul>
<b>%ExternalJavaLibDir%</b>	The folder where external, third-party Java libraries are located.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/java/lib/external</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/java/lib/external</li> </ul>
<b>%FILESERVER_EXE%</b>	The name of the executable for the File Server	<ul style="list-style-type: none"> <li>• On Windows: fileserver.exe</li> <li>• On Unix: boe_filesd</li> </ul>
<b>%HOARD_PATH%</b>	The location of the memory manager.	<ul style="list-style-type: none"> <li>• On Solaris: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/solaris_sparcv9/libhoard3.so</li> <li>• On other operating systems: This placeholder is blank.</li> </ul>
<b>%HOARD_PRELOAD%</b>	Specifies whether to preload the memory manager.	<ul style="list-style-type: none"> <li>• On Solaris: LD_PRELOAD_64</li> <li>• On other operating systems: This placeholder is blank.</li> </ul>
<b>%INSTALLROOTDIR%</b>	The folder where 64-bit Information platform services is installed.	Specified during installation
<b>%INSTALLROOTDIR32%</b>	The folder where 32-bit Information platform services is installed.	Specified during installation
<b>%IntroscopeAgentEnableInstrumentation%</b>	Indicates whether instrumentation for Java servers using Introscope Agent Enterprise Manager is enabled.	TRUE or FALSE, depending on whether Introscope Agent Enterprise Manager was enabled when Information platform services was installed

Placeholder	Description	Default values
<b>%IntroscopeAgentEnterpriseManagerHost%</b>	The Introscope Agent Enterprise Manager hostname to which instrumentation data is sent.	\$IntroscopeAgentEnterpriseManagerHost
<b>%IntroscopeAgentEnterpriseManagerPort%</b>	The Introscope Agent Enterprise Manager port to which instrumentation data is sent.	\$IntroscopeAgentEnterpriseManagerPort
<b>%IntroscopeAgentEnterpriseManagerTransport%</b>	The transport that is used when sending instrumentation data to the Introscope Agent Enterprise Manager. Allowed values are: <ul style="list-style-type: none"> <li>• TCP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SSL</li> </ul>	TCP
<b>%IntroscopeAgentEnterpriseManagerTransportHTTP%</b>	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through HTTP.	com.wily.isengard.postoffice hub.link.net.HttpTunnelingSocket Factory
<b>%IntroscopeAgentEnterpriseManagerTransportHTTPS%</b>	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through HTTPS.	com.wily.isengard.postoffice hub.link.net.HttpsTunnelingSocket Factory
<b>%IntroscopeAgentEnterpriseManagerTransportSSL%</b>	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through SSL.	com.wily.isengard.postoffice hub.link.net.SSLSocketFactory
<b>%IntroscopeAgentEnterpriseManagerTransportTCP%</b>	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through TCP.	com.wily.isengard.postoffice hub.link.net.DefaultSocketFactory
<b>%IntroscopeDir%</b>	The folder where Introscope Agent Enterprise Manager is installed.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/java/wily</li> <li>• On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enter prise_xi40/java/wily</li> </ul>

Placeholder	Description	Default values
<b>%JAVAW_EXE%</b>	The name of the executable for the Java Virtual Machine that has no console window.	<ul style="list-style-type: none"> <li>On Windows: javaw.exe</li> <li>On Unix: java</li> </ul>
<b>%JAVA_EXE%</b>	The name of the executable for the Java Virtual Machine.	<ul style="list-style-type: none"> <li>On Windows: java.exe</li> <li>On Unix: java</li> </ul>
<b>%JOBSEVERCHILD_EXE%</b>	The name of the executable for the Adaptive Job Server Child.	<ul style="list-style-type: none"> <li>On Windows: JobServerChild.exe</li> <li>On Unix: boe_jobcd</li> </ul>
<b>%JOBSEVER_EXE%</b>	The name of the executable for the Adaptive Job Server.	<ul style="list-style-type: none"> <li>On Windows: JobServer.exe</li> <li>On Unix: boe_jobsd</li> </ul>
<b>%JdkBinDir%</b>	The folder where the JDK binaries are located.	<ul style="list-style-type: none"> <li>On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/win64_x64/sapjvm/bin</li> <li>On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM64&gt;/sapjvm/bin</li> </ul>
<b>%JreBinDir%</b>	The folder where the JRE binaries are located.	<ul style="list-style-type: none"> <li>On Windows: &lt;IN STALLDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/win64_x64/sapjvm/jre/bin/</li> <li>On Unix: &lt;IN STALLDIR&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM64&gt;/sapjvm/jre/bin</li> </ul>
<b>%JVM_ARCH_ENVIRONMENT%</b>	Indicates whether the machine is running on a 32-bit or 64-bit JVM.	<ul style="list-style-type: none"> <li>On 32-bit Unix machines: -d32</li> <li>On 64-bit Unix machines: -d64</li> <li>On Windows: This placeholder is blank.</li> </ul>
<b>%JVM_HEADLESS_MODE%</b>	The command-line argument that specifies whether the JVM works in headless mode.	<ul style="list-style-type: none"> <li>On Windows: -Djava.awt.headless=false</li> <li>On Unix: -Djava.awt.headless=true</li> </ul>

Placeholder	Description	Default values
<b>%JM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%</b>	The command-line parameters that specify what the JVM does when it encounters Out of Memory errors.	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
<b>%JVM_IGNORE_CONSOLE_EVENTS%</b>	The command-line parameter that reduces the Java Virtual Machine's use of operating-system signals.	<ul style="list-style-type: none"> <li>Windows: -Xrs</li> <li>Linux: This placeholder is not available.</li> <li>Other operating systems: This placeholder is blank.</li> </ul>
<b>%JVM_SHARED_MEMORY_SEGMENT%</b>	The command-line parameters that enable JVM extensions and set the JVM's instance number.	<ul style="list-style-type: none"> <li>On Windows: "-Xjvms" "-XsapSystem:08"</li> <li>On Unix: This placeholder is blank.</li> </ul>
<b>%LANGUAGEPACKSDIR%</b>	The folder where the deployment's language packs are installed.	<ul style="list-style-type: none"> <li>On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/Languages/</li> <li>On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/Languages/</li> </ul>
<b>%LANGUAGEPACKSDIR32%</b>	The folder where the deployment's language packs are installed on 32-bit systems.	<ul style="list-style-type: none"> <li>On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/Languages/</li> <li>On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/Languages/</li> </ul>
<b>%LSTDir%</b>	The folder where LST configuration files are stored.	<ul style="list-style-type: none"> <li>On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/conf/lst</li> <li>On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/conf/lst</li> </ul>
<b>%MDAS_JVM_OS_STACK_SIZE%</b>	Specifies the JVM stack-size for the Multidimensional Analysis Service.	<ul style="list-style-type: none"> <li>On AIX: -Xmso1M</li> <li>Other operating systems: This placeholder is blank.</li> </ul>

Placeholder	Description	Default values
<b>%NCSInstrumentLevelThreshold%</b>	The threshold level of trace logging for the NCS library.	By default, this value is 0.
<b>%PAGESERVER_EXE%</b>	The name of the executable for the Crystal Reports 2011 Processing Server.	<ul style="list-style-type: none"> <li>On Windows: <code>crproc.exe</code></li> <li>On Unix: <code>boe_crprocd.bin</code></li> </ul>
<b>%PAGESERVER WRAPPED_EXE%</b>		<ul style="list-style-type: none"> <li>On Windows: <code>crproc.exe</code></li> <li>On Unix: <code>boe_crprocd</code></li> </ul>
<b>%PJSContainerDir%</b>	The folder where APS Container JARS are located.	<ul style="list-style-type: none"> <li>On Windows: <code>&lt;INSTALLEDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/java/pjs/container</code></li> <li>On Unix: <code>&lt;INSTALLEDIR&gt;/sap_bobj/enterprise_xi40/java/pjs/container</code></li> </ul>
<b>%PJSServicesDir%</b>	The folder where APS Service JARS are located.	<ul style="list-style-type: none"> <li>On Windows: <code>&lt;INSTALLEDIR&gt;/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services</code></li> <li>On Unix: <code>&lt;INSTALLEDIR&gt;/sap_bobj/enterprise_xi40/java/pjs/services</code></li> </ul>
<b>%Platform%</b>	The operating system on the machine running Information platform services	The operating system on the machine running Information platform services
<b>%Platform32%</b>	The 32-bit operating system of the machine running Business Intelligence platform	The 32-bit version of the operating system on the machine running Information platform services
<b>%PS_JVM_OS_STACK_SIZE%</b>	JVM Stack size for APS	<ul style="list-style-type: none"> <li>On AIX: <code>-Xmso1M</code></li> <li>On other operating systems, this placeholder is blank.</li> </ul>

Placeholder	Description	Default values
<b>%RasBinDir%</b>	The root folder of the Report Application Server.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/win32_x86</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM32&gt;/ras</li> </ul>
<b>%SERVER_FRIENDLY_NAME%</b>	The full name of the server.	The full name of the server
<b>%SERVER_NAME%</b>	The full name of the server.	The full name of the server
<b>%SMDAgentHost%</b>	The SMD Agent hostname to which instrumentation data is sent.	Specified during installation
<b>%SMDAgentPort%</b>	The SMD Agent port to which instrumentation data is sent.	Specified during installation
<b>%TRACE_CONFIGFILE_INI%</b>	The name and path of the <i>BO_trace.ini</i> file.	<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/conf/BO_trace.ini</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/conf/BO_trace.ini</li> </ul>
<b>%WarfilesDir%</b>		<ul style="list-style-type: none"> <li>• On Windows: &lt;IN <i>STALLDIR</i>&gt;/SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/</li> <li>• On Unix: &lt;IN <i>STALLDIR</i>&gt;/sap_bobj/enterprise_xi40/warfiles/webapps/</li> </ul>
<b>%WEBI_LD_PRELOAD%</b>	The name of the <i>LD_PRELOAD</i> environment variable for the platform.	<ul style="list-style-type: none"> <li>• On Linux: \$LD_PRELOAD\$:libmda_api.so:libmda_common.so</li> <li>• On other operating systems: \$LD_PRELOAD\$</li> </ul>

Placeholder	Description	Default values
<b>%WEBISERVER_EXE%</b>	The name of the executable for the Web Intelligence Processing Server.	<ul style="list-style-type: none"> <li>On Windows: wireportserv er.exe</li> <li>On Unix: WIReportServer</li> </ul>
<b>%WEBI_LD_PRELOAD_ONCE%</b>	The name of the <i>LD_PRELOAD_ONCE</i> environment variable for the platform.	<b>\$LD_PRELOAD_ONCE\$</b>
<b>%XCCACHE_EXE%</b>	The name of the executable for the Dashboards Cache Server.	<ul style="list-style-type: none"> <li>On Windows: xccache.exe</li> <li>On Unix: boe_xccached</li> </ul>
<b>%XCPROC_EXE%</b>	The name of the executable for the Dashboard Design Processing Server.	<ul style="list-style-type: none"> <li>On Windows: xcproc.exe</li> <li>On Unix: boe_xcprocd</li> </ul>

**Note:**

The following placeholders can be edited at the node level. Descriptions and default values can be found in the above table. Placeholders that do not appear in this list are read-only.

- **%DefaultAuditingDir%**
- **%DefaultDataDir%**
- **%DefaultLoggingDir%**
- **%IntroscopeAgentEnableInstrumentation%**
- **%IntroscopeAgentEnterpriseManagerHost%**
- **%IntroscopeAgentEnterpriseManagerPort%**
- **%IntroscopeAgentEnterpriseManagerTransport%**
- **%NCSInstrumentLevelThreshold%**
- **%SMDAgentHost%**
- **%SMDAgentPort%**
- **%WarfilesDir%**

**Related Topics**

- [To view and edit the placeholders for a node](#)

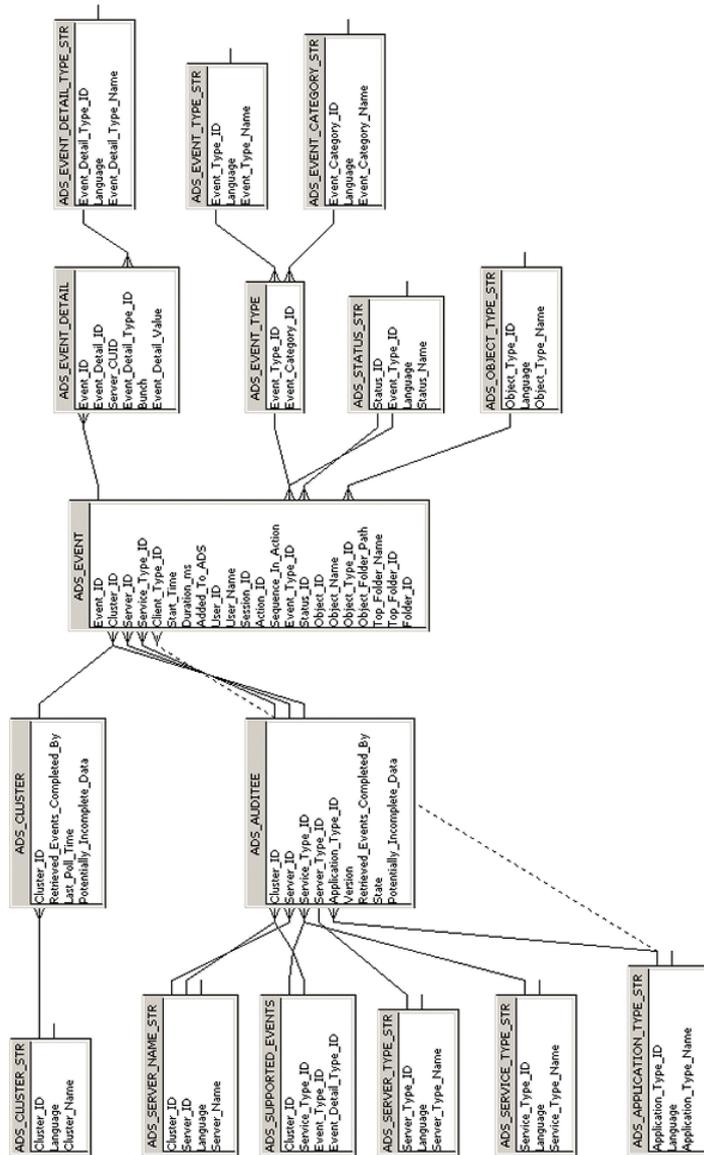


# **Auditing Database Schema Appendix**

## **21.1 Overview**

This appendix is a reference for any report designers that will be accessing and reporting off the Auditing Data Store tables. The following diagram and table explanations show you the tables where the auditing data will be recorded and how those tables are related.

## **21.2 Schema diagram**



## 21.3 Auditing Data Store Tables

### ADS\_EVENT table

This table records the basic properties for each event, central linking point for other tables in the schema.

Column Name	Field Type	Key	Description
Event_ID	Character (64)	Primary Key	A unique ID generated for the event.
Cluster_ID	Character (64)	Foreign key in ADS_Auditee table	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	Foreign key in ADS_Auditee table	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	Foreign key in ADS_Auditee table	<ul style="list-style-type: none"> <li>The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID.</li> <li>Client applications (BI launch pad or Interactive Analysis Rich Client for example) will record their application-type CUID.</li> </ul>
Client_Type_ID	Character (64)	Foreign key in ADS_Application_Type table	Records the Client Type ID of the client that established the session.
Start_Time	Datetime	NA	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	NA	Duration of operation in milliseconds.
Added_to_ADS	Datetime	NA	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	NA	The CUID of the user who performed the action.
User_Name	Character (255)	NA	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	NA	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	NA	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	NA	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.

Column Name	Field Type	Key	Description
Event_Type_ID	Integer	Foreign key in ADS_Event_type table	Type of event (View or Save, for example).
Status_ID	Integer	Foreign key in ADS_Status_Str table	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	NA	CUID of the object that the operation was performed on.
Object_Name	Character (255)	NA	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	Foreign key in ADS_Object_Type_Str Table	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	NA	The full folder path (for example Country/Region/City) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	NA	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	NA	Name of top level folder for the object. For example, if the object is located in Country/Region/City then Country will be recorded.
Top_Folder_ID	Character (64)	NA	The CUID of the top-level folder where the object resides. For example, if object is located in Country/Region/City then the CUID of the Country folder will be recorded.

### ADS\_EVENT\_DETAIL table

This table records event detail properties.

Column Name	Type	Key	Description
Event_Detail_ID	Integer	Primary Key	GUID for the event detail.
Event_ID	Character (64)	Foreign key in ADS_Event	Parent event GUID.

Column Name	Type	Key	Description
Event_Detail_Type_ID	Integer	Foreign key in ADS_Event_Detail_Str	Type of event detail.
Bunch	Integer	NA	<p>If the detail is part of a series, this is used to tie them together.</p> <p>For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of:</p> <ul style="list-style-type: none"> <li>• Prompt Name: Country</li> <li>• Prompt Value: USA</li> </ul> <p>Bunch 2 would consist of:</p> <ul style="list-style-type: none"> <li>• Prompt Name: State</li> <li>• Prompt Value: California</li> <li>• Prompt Value: Nevada</li> </ul>
Event_Detail_Value	Character (longtext)	NA	The value of the event detail.

### ADS\_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Column Name	Type	Key	Description
Cluster_ID	Character (64)	Primary Key	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	<ul style="list-style-type: none"> <li>• Primary Key</li> <li>• ADS_Server_Name_STR</li> </ul>	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	<ul style="list-style-type: none"> <li>• Primary Key</li> <li>• ADS_Service_Type_Str</li> <li>• ADS_Supported_Events</li> </ul>	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	ADS_Server_Type_Str	The server-type CUID for the server that triggered the event.

Column Name	Type	Key	Description
Application_Type_ID	Character (64)	ADS_Application_Type_Str	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	NA	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	NA	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee completed prior to this date/time are in the ADS.
State	Integer	NA	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	NA	Shows if this auditee may have events that were not transferred to the ADS.

#### ADS\_SERVER\_NAME\_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Column Name	Type	Key	Description
Cluster_ID	Character (64)	Primary Key	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	Primary Key	The CUID of the server.
Language	Character (10)	Primary Key	Code for the language of the server name; for example <i>EN</i> , or <i>DE</i> .
Server_Name	Character (255)	NA	The name of the server.

#### ADS\_SERVICE\_TYPE\_STR table

This table provides a multilingual dictionary of service-type names.

Column Name	Type	Key	Description
Service_Type_ID	Character (64)	Primary Key	The service-type or service-category CUID for the service.

Column Name	Type	Key	Description
Language	Character (10)	Primary Key	Code for the language the service-type name is recorded in, for example <i>EN</i> , or <i>DE</i> .
Service_Type_Name	Character (255)	NA	The name of the service-type.

### ADS\_APPLICATION\_TYPE\_STR table

This table provides a multilingual dictionary of client application-type names.

Column Name	Type	Key	Description
Application_Type_ID	Character (64)	Primary Key	The application-type CUID for the application.
Language	Character (10)	Primary Key	Code for the language in which the application type is recorded; for example <i>EN</i> , or <i>DE</i> .
Application_Type_Name	Character (255)	NA	The text name of the application type; Crystal Reports or Interactive Analysis for example.

### ADS\_SUPPORTED\_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Column Name	Type	Key	Description
Cluster_ID	Character (64)	Primary Key	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Primary Key	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	Foreign key in ADS_Event_Type	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	ADS_EVENT_DETAIL_TYPE_STR	CUID that identifies the type of event detail captured for that event (File Path, for example).

**ADS\_CLUSTER table**

This table records information on any clusters that contain Auditees.

Column Name	Type	Key	Description
Cluster_ID	Character (64)	<ul style="list-style-type: none"> <li>Primary Key</li> <li>ADS_Cluster_Str</li> </ul>	The GUID of the Cluster.
Retrieved_Events_Completed_By	Datetime	NA	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	NA	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	NA	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its <b>Potentially Incomplete Data</b> flag set, meaning that one auditee has events that haven't transferred to the ADS.

**ADS\_CLUSTER\_STR table**

This table provides a reference record of the different clusters in your deployment.

Column Name	Type	Key	Description
Cluster_ID	Character (64)	Primary Key	A unique ID of the cluster.
Language	Character (10)	NA	Code for the language setting for the cluster, for example, <i>EN</i> , or <i>DE</i> .
Cluster_Name	Character (255)	NA	The name of the cluster.

**ADS\_EVENT\_TYPE table**

This table provides a reference record for the different categories of events.

Column Name	Type	Key	Description
Event_Type_ID	Integer	Compound: <ul style="list-style-type: none"> <li>Primary Key</li> <li>ADS_Event_Type_Str</li> </ul>	The unique identifier for the type of event .
Event_Catagory_ID	Integer	ADS_Event_Catego-ry_Str table	Category of event. For example, common, Interactive Analysis, or Life-Cycle Management.

### ADS\_EVENT\_TYPE\_STR Table

This table provides a multilingual dictionary of event type names.

Column Name	Type	Key	Description
Event_Category_ID	Integer	Primary Key	The event-type ID for the event.
Language	Character (10)	Primary Key	Code for the language that the event category name is recorded in; for example <i>EN</i> , or <i>DE</i> .
Event_Type_Name	Character (255)	NA	The text name of the event type; View or Logon for example.

### ADS\_EVENT\_CATEGORY\_STR Table

This table provides a multilingual dictionary of event category names.

Column Name	Type	Key	Description
Event_Type_ID	Integer	Primary Key	The event-category ID.
Language	Character (10)	Primary Key	Code for the language that the event category name is recorded in; for example <i>EN</i> , or <i>DE</i> .
Event_Category_Name	Character (255)	NA	The name of the event category.

### ADS\_EVENT\_DETAIL\_TYPE\_STR table

This table provides a multilingual dictionary of event detail type names.

Column Name	Type	Key	Description
Event_Detail_ID	Integer	Primary Key	The event detail-type ID for the event detail.
Language	Character (10)	Primary Key	Code for the language that the event detail name is recorded in; for example <i>EN</i> , or <i>DE</i> .
Event_Detail_Type_Name	Character (255)	NA	The text name of the event detail type.

**ADS\_OBJECT\_TYPE\_STR Table**

This table provides a multilingual dictionary of event object names.

Column Name	Type	Key	Description
Object_Type_ID	Character (64)	Primary Key	Object-type CUID of the object
Language	Character (10)	Primary Key	Code for the language that the object type name is recorded in; for example <i>EN</i> , or <i>DE</i> .
Object_Type_Name	Character (255)	NA	Name of the object type.

**ADS\_STATUS\_STR Table**

This table provides a multilingual dictionary of event status names.

Column Name	Type	Key	Description
Status_ID	Integer	Primary Key	The numerical representation of the operation's status.
Event_Type_ID	Integer	Primary Key	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Primary Key	Code for the language that the event status is recorded in; for example <i>EN</i> , or <i>DE</i> .
Status_Name	Character (255)	NA	A text description of the event's status; Succeeded or Failed, for example.

**ADS\_EVENT\_DELETES**

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.



## More Information

Information Resource	Location
SAP product information	<a href="http://www.sap.com">http://www.sap.com</a>
SAP Help Portal	<p><a href="http://help.sap.com/businessobjects">http://help.sap.com/businessobjects</a></p> <p>Access the most up-to-date English documentation covering all SAP BusinessObjects products at the SAP Help Portal:</p> <ul style="list-style-type: none"> <li>• <a href="http://help.sap.com/bobi">http://help.sap.com/bobi</a> (Business Intelligence)</li> <li>• <a href="http://help.sap.com/boepm">http://help.sap.com/boepm</a> (Enterprise Performance Management)</li> <li>• <a href="http://help.sap.com/boeim">http://help.sap.com/boeim</a> (Enterprise Information Management)</li> </ul> <p>Certain guides linked to from the SAP Help Portal are stored on 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> <p>To find a comprehensive list of product documentation in all supported languages, visit: <a href="http://help.sap.com/boall">http://help.sap.com/boall</a>.</p>
SAP Support Portal	<p><a href="http://service.sap.com/bosap-support">http://service.sap.com/bosap-support</a></p> <p>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.</p>
Developer resources	<p><a href="http://www.sdn.sap.com/irj/sdn/bi-sdk-dev">http://www.sdn.sap.com/irj/sdn/bi-sdk-dev</a></p> <p><a href="https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary">https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary</a></p>
SAP BusinessObjects articles on the SAP Community Network	<p><a href="http://www.sdn.sap.com/irj/boc/articles">http://www.sdn.sap.com/irj/boc/articles</a></p> <p>These articles were formerly known as technical papers.</p>

Information Resource	Location
Notes	<a href="https://service.sap.com/notes">https://service.sap.com/notes</a> These notes were formerly known as Knowledge Base articles.
Forums on the SAP Community Network	<a href="https://www.sdn.sap.com/irj/scn/forums">https://www.sdn.sap.com/irj/scn/forums</a>
Training	<a href="http://www.sap.com/services/education">http://www.sap.com/services/education</a> From traditional classroom learning to targeted e-learning seminars, we can offer a training package to suit your learning needs and preferred learning style.
Consulting	<a href="http://www.sap.com/services/bysubject/businessobjectsconsulting">http://www.sap.com/services/bysubject/businessobjectsconsulting</a> 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

## A

- access 69
  - groups 60
  - inboxes 61
  - server groups 305
  - servers 305
  - users 60
- access control lists
  - adding principals to 79
  - viewing 79
- access levels 69, 78, 92
  - administration 92
  - assigning to principals 79
  - copying 86
  - creating 87
  - deleting 87
  - managing across sites 89
  - modifying rights in 88
  - predefined 83
  - RAS 306
  - relationships to objects 89
  - renaming 87
  - rights 487
  - tasks, rights required for 83
  - view vs. view on demand 85
  - viewing 79
- accounts
  - managing 47, 52
  - SAP BusinessObjects Enterprise 228
- active trust relationship 99
- Adaptive Job Server 29, 492, 520
  - command-line options 478
- Adaptive Processing Server 29, 408, 492
- adding 298
  - cluster members 298
  - CMS 300
  - servers 295
  - subgroups 55
  - users to groups 57
- administration
  - assigning rights 279
  - delegating 92
  - groups 60
  - inboxes 61
  - rights 92
  - servers and server groups 305
  - users 60
- advanced rights 70, 78, 80
- affinity, and SSL 100
- Agent Builder 417
- Alerting
  - rights 488
- aliases
  - assigning to users 66
  - creating 66
    - for existing users 66
    - for new users 65
  - deleting 67
  - disabling 67
  - managing 65
- anonymous single sign-on 164
- application tier 309
- architecture 19, 404
- architecture diagram 19
- attributes, logon tokens 99
- auditing
  - architecture 425
  - auditing data store
    - schema diagram 537
    - schema tables 538
  - CMC page 431
  - common events 445
  - configuring 431
  - database connection settings 435
  - event detail ID 445, 454, 456
  - event details 445, 454, 456
  - event properties 445, 456
  - event types 445
    - auditing modification 454
    - custom access level modified 454
    - rights modification 454
    - rollback 456
    - VMS add 456
    - VMS checkin 456
    - VMS checkout 456
    - VMS export 456
    - VMS lock 456
    - VMS retrieve 456
    - VMS unlock 456
  - event types:create 445
  - event types:delete 445
  - event types:deliver 445
  - event types:edit 445
  - event types:logon 445
  - event types:logout 445
  - event types:modify 445
  - event types:prompt 445
  - event types:retrieve 445
- auditing (*continued*)
  - event types:run 445
  - event types:save 445
  - event types:search 445
  - event types:trigger 445
  - event types:view 445
  - event-type ID 445, 454, 456
  - events
    - configuring 433
    - database retention 435
    - list of 436
    - properties and details 436
  - information flow 425
  - lifecycle management console
    - events 456
  - metrics 431
  - platform events 454
  - status summary 431
  - web activity 103
- authentication 24
  - enterprise 166
  - LDAP 180, 181
  - primary 162
  - security plug-ins 163
  - Trusted Authentication 169
  - types 50
  - Web Application Container Server (WACS) 356
  - Windows AD 196
- authorizations
  - for SAP BusinessObjects Enterprise 228
- automatically starting servers 293

## B

- backing up BI platform
  - hot backup:to enable 374
- backing up the BI platform
  - hot backup prerequisites 373
- BI launch pad
  - configuring 61
  - group preferences 62, 63
  - logon 61
- BIAR Command-Line Tool 385
- BIAR Engine Command-Line Tool 396, 401
  - BIAR Engine Command-Line Tool 393
- BOE war file 61
- BOLMT 44, 289

- breach time 406
- browser-based clients 37
- Business Process BI Service
  - adding to a Web Application Container Server 350
  - removing from a Web Application Container Server 350

## C

- CA Wily Introscope 26
- cacert.der 117
- cakey.pem 117
- categories 63
  - rights 484
- CCM
  - adding a server 295
  - deleting a server 298
  - enabling and disabling servers 294, 295
  - nodes 320
    - adding 322
    - deleting 328
    - moving 332
    - recreating 325
    - renaming 330
    - user credentials, changing for 340
  - restarting the system 293
  - starting, stopping, and restarting servers 291, 293
- Central Configuration Manager (CCM) 16, 37
- Central Management Console (CMC) 15, 38
- Central Management Server 29
- Central Management Server. See CMS. 227
- certificate files 117, 352
- certificate trust lists 353
- ClearCase 27
- clients
  - desktop 37
  - web 37
- clients, browser-based 38
  - Central Management Console (CMC) 15, 38
- clients, desktop
  - Central Configuration Manager (CCM) 16, 37
  - Upgrade management tool 16, 37
- cloning
  - servers 296, 297
  - Web Application Container Servers (WACS) 349

- cluster keys 108
  - dbinfo file 108
  - overview 108
  - resetting on UNIX 110
  - resetting on Windows 109
- cluster support 407
- clusters 298, 300
  - adding a CMS 300
  - changing names 301
  - nodes 298
  - viewing details 307
- CMC
  - cloning servers 296, 297
  - cryptographic keys 112
  - deleting a server 298
  - enabling and disabling servers 294, 295
  - managing servers 283
  - rights 487
  - starting, stopping, and restarting servers 291, 292
  - Windows server dependencies, adding 340
- CMS 227, 243, 408
  - adding to a cluster 300
  - as nameserver 318, 319
  - authentication 162
  - changing cluster name 301
  - clustering 298, 300
    - installing new cluster member 300
    - requirements 298
  - command-line options 477
  - configuring 318, 319
  - default port 318, 319
  - distributed security 100
  - enabling and disabling other servers 294, 295
  - metrics 307
  - properties 492
  - session variables 100
    - authentication 162
    - tracking 101
  - starting 294
  - stopping 294
  - troubleshooting 294
  - troubleshooting multihomed machines 318
- command-line options 475
  - Adaptive Job Server 478
  - all servers 475
  - CMS 477
  - Input and Output File Repository Servers 479
  - SSL 116

- communication 162
  - between browser and Web application server 162
  - between Information platform services servers 123
- configuration 412
- configuration mode 249
- configuration templates 310
  - applying 311
  - best practices 310
  - restoring system defaults 312
  - setting 311
- configuring
  - Apache 2.2 154
  - application tier 309
  - clusters 298
  - CMS clusters 301
  - configuration templates 311
  - firewalls 133
  - intelligence tier 309
  - ISA 2006 155
  - multiple servers 310
  - nodes 298
  - processing tier 309
  - reverse proxy servers 152, 153
  - Trusted Authentication 170
  - WebSEAL 6.0 154
- configuring auditing, see auditing 431
- Connectivity 420
- cookies 100
  - logon tokens 99
  - session tracking 100
- copying
  - access levels 86
- creating
  - access levels 87
  - groups 54
  - server subgroups 304
  - user accounts 52
- cryptographic keys 108
  - CMC 112
  - create new 114
  - mark as compromised 115
  - object list 114
  - revoking 115
  - status 113
- cryptographic officers 111
  - adding members 111
- CTS Transport (CTS+) 26

## D

- daemons, signal handling 476
- Dashboard 403
- Dashboard Analytics Server 492
- Dashboard Server 492

- data
  - live 85
  - saved 85
- data security
  - backward compatibility 106
  - cluster keys 108
  - cryptographic keys 108
  - cryptography 108
  - default data processing mode 106
  - encryption keys 108
  - FIPS-compliant mode 106
  - overview 105
  - two-key cryptography 105
- databases 20
  - single sign-on access 165
- default settings
  - ports 318, 319
  - servers 312
- delegated administration 92
- deleting
  - access levels 87
  - aliases 67
  - groups 56
  - servers 298
  - user accounts 54
  - Web Application Container Servers (WACS) 349
- DES encryption 200
- desktop clients 37
- destination sites
  - access levels 89
- diagram, architecture 19
- directory servers 181
  - about LDAP 180
  - security plug-in 181
- disabling
  - aliases 67
  - guest accounts 57
  - servers 294, 295
- disaster recovery planning 97
- dynamic-link libraries, processing
  - extensions 105

## E

- effective rights 78
- enabling
  - servers 294, 295
- encoding, logon tokens 99
- end-to-end single sign-on 165
- entitlement systems 229
- Event Log 308, 340
- Event Server 408, 492
- execution mode 249
- extensions, processing 105

## F

- federation
  - access levels 89
- File Repository Servers 29, 492
  - command-line options 479
- FIPS-compliant mode
  - Federal Information Processing Standard 106
  - security setting 106
  - turning off Windows 107
  - turning on Unix 107
  - turning on Windows 106
- firewalls 102
  - configuration
    - SAP integration 143
  - configuration scenarios 138
  - configuring 133
    - for Oracle E-Business integration 147
    - JD Edwards EnterpriseOne integration 145
    - PeopleSoft Enterprise integrations 148
    - Siebel integration 150
  - debugging 136, 137
  - forcing servers to register by name 320
  - server communications, and 123
  - Web Application Container Server (WACS) 366
- folder inheritance 73
  - rights override 74
- folders
  - object rights
    - inheritance 73
  - rights 484

## G

- global system metrics 307
- groups 236
  - adding subgroups 55
  - adding users to 57
  - assigning rights to 79
  - BI launch pad preferences 62
  - checking rights for 81, 82
  - creating 54
  - cryptographic officers 111
  - default 49
  - deleting 56
  - granting access to 60
  - managing 49
  - mapping 244, 261, 267, 273
  - modifying 55

- groups (*continued*)
  - rights 486
    - breaking inheritance 90
    - inheritance 71
    - on top-level folders 81
    - rights override 74
    - specifying group membership 56
    - viewing
      - members 55
      - rights for 79
- Guest accounts
  - disabling 57

## H

- hosts
  - configuring LDAP 182, 187
- hosts file, configuring for NAT firewall 135
- hot backup 373
- HTTP 100, 162
- HTTPS
  - configuring Web Application Container Servers (WACS) 351, 354, 365

## I

- Import Wizard
  - see Upgrade management tool 16, 37
- inboxes
  - controlling access to 61
- Information platform services
  - architecture diagram 19
  - communication between servers 123
  - deployment with reverse proxy servers 151, 152
  - disaster recovery planning 97
  - importing roles 236
  - mapping roles 267
  - primary authentication process 162
  - rights 69
  - security recommendations 98
  - top-level folders, rights 81
  - Web Application Container Server (WACS) 343
- Information platform services SDK 105
- Information platform services servers 416
  - configure Kerberos and browsers 203, 357
  - configuring hosts file for firewall 135

inheritance 71  
     breaking 90  
     folder 73  
     group 71  
     limiting 75  
     rights override 74  
 Input File Repository 29, 408, 492  
 installation directory, location 321  
 INSTALLDIR 14  
 integration  
     SAP 26  
 intelligence tier 309  
 Interactive Analysis Processing Server 29  
 internationalization 23  
 Introscope 420  
 IPv6  
     CMC 313  
     options 313  
     setting address in CMC 314  
 ISA 2006  
     configuring for Oracle 10gR3 158  
     configuring for Sun Java 8.2 158  
     configuring for Tomcat 5.5 158  
     configuring for WebSphere CE 2.0 158

## J

JAAS, configuration file 206, 207, 358  
 Java application server, Kerberos 203  
 Java Management Extensions (JMX) 404  
 Java, Kerberos 209  
 JD Edwards EnterpriseOne integration  
     firewall configuration 145  
 JMX MBeans 417  
 JMX Remote API 415

## K

Kerberos 203, 357  
     configuration file 204, 205, 358  
     Krb5.ini 206, 359  
     single sign-on for Java 363, 364  
     single sign-on for Java InfoView 210  
     troubleshooting 225, 360  
 Kerberos configuration 203  
 key files 117  
 KPIs (key performance indicators) 403  
 Krb5.ini 206, 359

## L

languages 23  
 LCM settings 385  
 LCM Version Management System settings 385  
 LDAP  
     accounts 180  
         troubleshooting 196  
     authentication 180  
         configuring 181  
     authentication plug-in 181  
     configuring single sign-on 190  
     groups  
         mapping 192  
     hosts  
         configuring 182, 187  
         managing multiple 185  
     mapping against Windows AD 194  
     Secure Sockets Layer (SSL) 180  
     security plug-in 181  
 license audit 44, 289  
     procedure 45, 289  
 license key 44, 288  
     adding 43, 288  
     measuring usage 44, 289  
     overview 43, 287  
     purchasing 43, 287  
     viewing 43, 287  
 Life Cycle Management  
     BIAR Engine Command-Line Tool 396  
 Lifecycle management (LCM) 27  
 lifecycle management console  
     BIAR Command-Line Tool 385  
     BIAR Engine Command-Line Tool 401  
 Lightweight Directory Access Protocol.  
     See LDAP 180  
 limiting  
     scope of rights 75  
 live data 85  
 Live Office  
     configuration for reverse proxy servers 157  
 load balancing 100  
     adding a CMS 300  
     and distributed security 100  
     clustering 298  
     Web Application Container Servers (WACS) 364  
 localization 23  
 log on  
     BI launch pad 61  
     protection against malicious attempts 103

logging 308  
     server activity 308  
     web activity 103  
 logon  
     workflow 39  
 logon tokens 99  
     authentication 162  
     distributed security 100  
     session tracking 100  
 logon.csp 162

## M

managed objects 250  
     Information platform services group 250, 254  
     PeopleSoft roles 250, 254  
     universes 250, 255  
 mapped users, managing aliases 65  
 mapping roles 236, 244, 261, 267, 273  
 MBeans 404  
 memory settings  
     changing on a Web Application Container Server (WACS) 368  
 metric 406  
 metrics  
     viewing 307  
 Monitoring 403  
 Monitoring Agent 417  
 Monitoring Data Categories 417  
 monitoring server 407  
 monitoring service 412  
 multihomed computers  
     Web Application Container Server (WACS) 366  
 multihomed machines 315, 316

## N

navigation tree  
     servers 283  
 Network Address Translation  
     configuring, server hosts file 135  
 network interface  
     troubleshooting multiple 316  
 networking environments  
     IPv4  
         dual IPv4/IPv6 nodes 313  
     IPv6 313  
 node management scripts, location 321  
 node placeholders 523  
 nodes 29, 320  
     adding 321, 335  
         a CMS 300  
         AddNode.bat 323

nodes (*continued*)  
 adding (*continued*)  
   addnode.sh 324  
   CCM 322  
   new machine 322  
   serverconfig.sh 323  
   to a cluster 300  
 clustering 298  
 CMC 283  
 deleting 328, 335  
   CCM 328  
   serverconfig.sh 329  
 moving 331, 337  
   CCM 332  
   MoveNode.bat 332  
   movenode.sh 334  
   serverconfig.sh 333  
 recreating 335  
   AddNode.bat 326  
   addnode.sh 327  
   CCM 325  
   RemoveNode.bat 328  
   removenode.sh 329  
   scenarios for 325  
   serverconfig.sh 326  
 renaming 330  
   CCM 330  
   serverconfig.sh 331  
 non-primary network interface 316  
 notes, rights 485  
 notification 404  
 notification delivery 406  
 number of logons, logon tokens 99  
 number of minutes, logon tokens 99

## O

objects  
   rights 481  
   setting 79  
   viewing 79  
 Oracle  
   JAAS 206  
   Java options 209  
   Kerberos 204  
 Oracle E-Business Suite  
   mapping roles to SAP  
     BusinessObjects Enterprise  
     273  
 Oracle E-Business Suite integration  
   firewall configuration 147  
 Oracle EBS  
   update aliases 277  
   update roles 277  
 origin sites  
   access levels 89

Output File Repository 29, 408, 492  
 owner rights 95

## P

passwords  
   changing 59  
     options 59, 168  
   restrictions 103  
 PeopleSoft Enterprise integration  
   firewall configuration 148  
 PeopleSoft EPM Security Bridge  
   response file 251  
 PeopleSoft response file 255  
   parameters 256  
 performance 403  
   clusters 298  
   load balancing 100  
 Permissions Explorer 79  
 placeholders 523  
 Platform Java Server 404  
 PLATFORM64DIR 14  
 PlatformServices.properties 300  
 plug-ins  
   security 24  
 plug-ins, security 163  
 PM Repository Server 408  
 port numbers  
   changing 318, 319  
   conflicts 368  
   Web Application Container Server  
     (WACS) 367  
 primary authentication 162  
 primary network interface 316  
 principals  
   assigning advanced rights to 80  
   assigning rights to 79  
   checking rights for 81, 82  
   rights, on top level folders 81  
   viewing rights for 79  
 probe 406  
 Probe 403  
 processing extensions 105  
 processing tier 309  
 publishing, assigning rights for 280

## Q

queries  
   security 81, 82

## R

registry keys 191

relationship queries  
   for access levels 89  
 Remote Method Invocation (RMI) 404  
 Remote Procedure Call 340  
 renaming, access levels 87  
 Report Application Server  
   required object rights 306  
 report objects  
   rights for creating/modifying 306  
 requirements  
   clustering 298  
 response file 251  
   applying 253  
   creating 251  
 response time 403  
 restarting servers 291, 292, 293  
 restore  
   system defaults 312, 369  
 restrictions 104  
   guest account 104  
   logon 104  
   password 103  
   user 104  
 reverse proxy servers  
   configuring Apache 2.2 154  
   configuring ISA 2006 155  
   configuring WebSEAL 6.0 154  
   configuring with Information  
     platform services 152, 153  
   deployment with a Web Application  
     Container Server (WACS) 365  
   deployment with Information  
     platform services 151, 152  
   Live Office 159, 160  
   session cookies 158  
   special configuration 157  
   supported 152  
   Tomcat 157  
   using with Web Application  
     Container Servers (WACS) 365  
   viewer URL 159, 160  
   web services 157  
 rights 69, 279, 481  
   access levels 69, 487  
     managing across sites 89  
     modifying included rights 88  
     relationship queries 89  
     replicated 89  
     tasks 83  
   administration 92, 95  
   administration rights 279  
   advanced rights 70, 80  
   Alerting 488  
   assigning to principals 79  
   categories 484  
   CMC 487

- rights (*continued*)
  - effective rights 78
  - folders 484
  - general 481
  - groups 60, 486
  - inboxes 61
  - inheritance 71
    - breaking 90
    - folder 73
    - group 71
  - limiting scope of 75
  - managing 78
  - notes 485
  - owner rights 95
  - publishing rights 280
  - Report Application Server 306
  - rights override 74
  - scope of rights 75
  - security query 81, 82
  - server groups 305
  - servers 305
  - top-level folders 81
  - type-specific 76
  - users 60, 486
  - view vs. view on demand 85
  - viewing 79
- RMI protocol 412
- roles 244, 261, 267, 273
  - assigning rights to 279
  - importing 236
  - mapping 236, 244, 247, 261, 263, 267, 273
  - remapping 269
  - unmapping 247, 278
- row-level security, processing
  - extensions 105

## S

- SAML
  - SSO 171
- SAP
  - firewall configuration 143
  - integration 26
  - updating aliases 238
  - updating roles 238
- SAP Authentication 227
  - CMC options 231
- SAP BusinessObjects Enterprise
  - administration rights 279
  - creating account for 228
  - mapping roles 244, 261, 273
  - publishing rights 280
  - traces 461
- SAP Solution Manager 26
  - saved data 85
- scope of rights 75
- script parameters, nodes
  - adding 335
  - deleting 335
  - moving 337
  - recreating 335
- SCRIPTDIR 14
- Secure Sockets Layer (SSL) 102, 116, 119, 120, 180
  - and LDAP 180
  - and load balancing 100
- security 24, 249, 279
  - active trust relationship 99
  - applying 253
  - auditing web activity 103
  - customizing rights 279
  - distributed 100
  - environment protection 101
  - firewalls 102
  - Guest account restrictions 104
  - importing settings 250
  - logon restrictions 104
  - managing 78
  - managing settings 254
  - password restrictions 103
  - plug-ins 24, 163
  - processing extensions 105
  - protection against malicious logon
    - attempts 103
  - queries 81, 82
  - restrictions 104
  - session tracking 100
  - top level folders 81
  - user restrictions 104
  - web browser to web server 102
  - web servers 101
- security plug-ins 163, 227
  - LDAP authentication 181
  - Windows AD authentication 197
- server dependencies
  - adding 340
  - Event Log 340
  - Remote Procedure Call 340
- server groups
  - access to 305
  - creating 303
  - nodes 283
  - subgroups 304
  - subgroups of servers 302, 304
- Server Intelligence Agent
  - nodes 320, 321, 325, 328, 330
    - adding 322, 323, 324, 335
    - deleting 328, 329, 335
    - moving 331, 332, 333, 334, 337
    - new machine, adding to 322

- Server Intelligence Agent (*continued*)
  - nodes (*continued*)
    - recreating 325, 326, 327, 328, 329, 335
    - renaming 330, 331
    - user credentials, changing for 340
  - starting servers automatically 293
  - Windows server dependencies,
    - adding 340
- Server Intelligence Agent (SIA)
  - shutdown workflow 40
  - start-up workflow 39
- server metrics 505
  - Adaptive Job Server Metrics
    - Children 520
    - Comm. Failures 520
    - Concurrent Jobs 520
    - Email Destination Default Settings Valid 520
    - Failed Job Creations 520
    - File System Destination Default Settings Valid 520
    - FTP Destination Default Settings Valid 520
    - Inbox Destination Default Settings Valid 520
    - Initializing 520
    - Maximum Concurrent Jobs Allowed 520
    - Maximum Jobs Allowed 520
    - Peak Jobs 520
    - PID 520
    - Received Job Requests 520
    - Scheduling Service 520
    - Scheduling Services 520
    - Shutting Down 520
    - Temporary Directory 520
  - Adaptive Processing Server metrics
    - Auditing Events Received 513
    - Available Processors 513
    - CPU Usage Percentage (last 15 minutes) 513
    - CPU Usage Percentage (last 5 minutes) 513
    - Cube Count 513
    - Data Federation Service is available 513
    - DSLServiceMetrics.activeConnectionCount 513
    - DSLServiceMetrics.activeOLAPConnectionCount 513
    - DSLServiceMetrics.activeSessionCount 513
    - DSLServiceMetrics.queryCount 513
    - Free Memory (MB) 513
    - Indexing Running 513
    - JVM Deadlocked Threads Counter 513
    - JVM Debug Info 513
    - JVM Lock Contention Count 513
    - JVM Trace Flags 513

server metrics ( <i>continued</i> )	server metrics ( <i>continued</i> )	server metrics ( <i>continued</i> )
Adaptive Processing Server metrics ( <i>continued</i> )	Adaptive Processing Server metrics ( <i>continued</i> )	Central Management Service metrics ( <i>continued</i> )
JVM Version Info 513	Total Records Transferred from Data Sources 513	Product Version 508
Last Content Store Generation Timestamp 513	Transport Layer Thread Pool Size 513	Resource Version 508
Last Index Update Timestamp 513	Central Management Service metrics	Running Jobs 508
Maximum Memory (MB) 513	Auditing Database Connection Name 508	System Database Connection Name 508
Number of Active Connections to Loaded Connectors 513	Auditing Database Last Updated On 508	System Database Server Name 508
Number of Active Threads 513	Auditing Database User Name 508	System Database User Name 508
Number of Connections 513	Auditing Thread Last Polling Duration Cycle (seconds) 508	Waiting Jobs 508
Number of Documents Indexed 513	Auditing Thread Utilization 508	File Repository Server metrics
Number of failed extraction attempts since service start 513	Average Commit Response Time Since Startup (msec) 508	Active Connections 512
Number of Failed Queries 513	Average Query Response Time Since Startup (msec) 508	Active Files 512
Number of Full GCs 513	Build Date 508	Available Disk Space in Root Directory (%) 512
Number of Loaded Connectors 513	Build Number 508	Available Disk Space in Root Directory (GB) 512
Number of page faults during GC (last 15 minutes) 513	Clustered CMS Servers 508	Data Sent (MB) 512
Number of page faults during GC (last 5 minutes) 513	CMS Auditor 508	Data Written (MB) 512
Number of Queries Consuming Memory 508	Completed Jobs 508	Free Disk Space in Root Directory (GB) 512
Number of Queries in Query Analyze Step 513	Concurrent User Licenses 508	List of Active Files 512
Number of Queries in Query Execution Step 513	Connection to Auditing Database is Established 508	Total Disk Space in Root Directory (GB) 512
Number of Queries in Query Optimization Step 513	Currently Used System Database Connections 508	Web Application Container Server metrics
Number of Queries Using Disk 513	Data Source Name 508	List of Running WACS Connectors 519
Number of Queries Waiting for Resources 513	Established System Database Connections 508	WACS Connector(s) Failed at Startup 519
Number of Running Queries 513	Existing Concurrent User Accounts 508	Server metrics
Number of Successful Extraction Attempts since the Service Start 513	Existing Named User Accounts 508	viewing 307
Percentage of stopped system during GC (last 15 minutes) 513	Failed Jobs 508	Server metrics About
Percentage of stopped system during GC (last 5 minutes) 513	Longest Commit Response Time Since Startup (msec) 508	Auditing Metrics
Query Count 513	Longest Query Response Time Since Startup (msec) 508	Current Number of Auditing Events in the Queue 505
Service Available 513	Named User Licenses 508	common metrics
Services 513	Number of Commits Since Startup 508	Busy Server Threads 505
Session Count 513	Number of Logons Since Startup 508	CPU Type 505
Threads in Transport Layer 513	Number of Objects in CMS System Cache 508	CPUs 505
Total Bytes of Disk Used by Query Execution 513	Number of Objects in CMS System DB 508	Disk Size (GB) 505
Total Bytes of Memory Used by Metadata Cache 513	Number of Queries Since Startup 508	Host IP Address 505
Total Bytes of Memory Used by Query Execution 513	Number of Sessions Established by All Users 508	Host Name 505
Total Bytes Produced by Query Execution 513	Number of Sessions Established by Concurrent Users 508	Local Time 505
Total Bytes Transferred from Data Sources 513	Number of Sessions Established by Named Users 508	Logging Directory 505
Total Memory (MB) 513	Number of Sessions Established by Servers 508	Machine Name 505
Total Records Produced by Query Execution 513	Peak Number of User Sessions Since Startup 508	Name Server 505
	Pending Jobs 508	Operating System 505
	Pending System Database Requests 508	PID 505
		RAM (MB) 505
		Registered Name 505
		Request Port 505
		Used Disk Space (GB) 505
		Version 505
		server placeholders 523
		server properties 489
		server states 283
		server types 34, 35

- serverconfig.sh
  - nodes
    - adding 323
    - deleting 329
    - moving 333
    - recreating 326
    - renaming 331
- servers 21
  - access to 305
  - activity, logging 308
  - adding 295
  - Auto Reconnect to System
    - Database 492
  - Bind to All IP Addresses 492
  - Bind to Hostname or IP Address 492
  - bscLogin.conf File Location 492
  - Certificate Alias 492
  - Certificate Store File Location 492
  - Certificate Store Type 492
  - Certificate Trust List File Location 492
  - Certificate Trust List Private Key
    - Access Password 492
  - changing 290
    - state 290
    - status 291
  - Cleanup Interval 492
  - cloning 296, 297
  - command lines 475
  - Common Server Properties
    - Auto Assign 489
    - Automatically start this server
      - when the SIA starts 489
    - Host Identifiers 489
    - Log Level 489
    - Request Port 489
    - Restore System Defaults 489
    - Set Configuration Template 489
    - Use Configuration Template 489
  - communication 123
  - configuration templates 310
    - applying 311
    - setting 311
  - configuring 309
  - configuring servers to use service
    - account 203
  - contrast with services 29
  - Core Services Properties
    - Auto Reconnect to System
      - Database 492
    - Bind to All IP Addresses 492
    - Bind to Hostname or IP
      - Address 492
    - bscLogin.conf File Location 492
- servers (*continued*)
  - Core Services Properties
    - (*continued*)
    - Certificate Alias 492
    - Certificate Store File Location 492
    - Certificate Store Type 492
    - Certificate Trust List File
      - Location 492
    - Certificate Trust List Private
      - Key Access Password 492
    - Cleanup Interval 492
    - Enable Client Authentication 492
    - Enable HTTP through Proxy 492
    - Enable HTTPS 492
    - Event Poll Interval 492
    - File Store Directory 492
    - HTTP Port 492
    - HTTPS Port 492
    - Idle Connection Timeout 492
    - Idle Transient Object Timeout 492
    - Krb5.ini File Location 492
    - Log level 492
    - Maximum Child Requests 492
    - Maximum Concurrent Jobs 492
    - Maximum Concurrent Requests 492
    - Maximum HTTP Header Size 492
    - Maximum Idle Time 492
    - Maximum Retries for File
      - Access 492
    - Maximum Try 492
    - Name Server Port 492
    - Port 492
    - Port Offset 492
    - Private Key Access Password 492
    - Protocol 492
    - Proxy Hostname 492
    - Proxy Port 492
    - Service Startup Timeout 492
    - Single Sign-On Expiry 492
    - System Database Connections
      - Requested 492
    - Temporary Directory 492
    - URL For Monitoring Agent 492
    - Visualization Engine Cleanup
      - Timeout (in seconds) 492
    - Visualization Engine Swap
      - Timeout (in seconds) 492
  - default settings 312
  - deleting 298
- servers (*continued*)
  - disabling 294, 295
  - Enable Client Authentication 492
  - Enable HTTP through Proxy 492
  - Enable HTTPS 492
  - enabling 294, 295
  - Event Poll Interval 492
  - File Store Directory 492
  - granting service account rights
    - 201, 202
  - grouping 302
  - host identification options 313
  - hostname 314
  - HTTP Port 492
  - HTTPS Port 492
  - Idle Connection Timeout 492
  - Idle Transient Object Timeout 492
  - IPv6 address 314
  - Krb5.ini File Location 492
  - list 283
  - Log level 492
  - logging activity 308
  - Maximum Child Requests 492
  - Maximum Concurrent Jobs 492
  - Maximum Concurrent Requests 492
  - Maximum HTTP Header Size 492
  - Maximum Idle Time 492
  - Maximum Retries for File Access 492
  - Maximum Try 492
  - modifying group membership 305
  - Name Server Port 492
  - navigation tree 283
  - nodes 29
  - performance settings 309
  - placeholders 297
  - Port 492
  - Port Offset 492
  - Private Key Access Password 492
  - properties 309, 310
  - Protocol 492
  - Proxy Hostname 492
  - Proxy Port 492
  - registering by name 320
  - restarting 291, 292, 293
  - Service Startup Timeout 492
  - set IP address 314
  - setting service account 200
  - Single Sign-On Expiry 492
  - standard command-line options 475
  - starting 291, 292, 293
    - automatically 291, 292
  - state 290
  - status 283

- servers (*continued*)
  - stopping 291, 292, 293
  - System Database Connections
    - Requested 492
  - Temporary Directory 492
  - UNIX signal handling 476
  - URL For Monitoring Agent 492
  - viewing a server's status 291
  - Visualization Engine Cleanup
    - Timeout (in seconds) 492
  - Visualization Engine Swap Timeout
    - (in seconds) 492
- service account
  - configuring servers 203
  - delegation 200
  - setting up 200
- service account rights 201
  - granting 202
- service categories 33, 283
- services 31
  - configuration templates 310
  - contrast with servers 29
- session variables 100
  - authentication 162
- sessions 100
  - tracking 100
- settings
  - top-level folder rights 81
- shared libraries, as processing
  - extensions 105
- SI\_AVAILABILITY\_PROPERTY 407
- Siebel integration
  - configuring firewalls 150
- signal handling 476
- single sign-on 24, 164, 219, 227
  - anonymous 164
  - authentication
    - Windows AD 199
  - end-to-end 165
  - importing roles 236
  - Kerberos 210, 363, 364
  - service account 211
  - setting up
    - LDAP 190
    - SiteMinder 190, 219
    - Windows AD 199
  - to database 165
  - to Information platform services
    - 164
  - troubleshooting 191
- SiteMinder
  - BOE war configuration 191
  - configuring LDAP plug-in 190
  - error 191
  - setting up single sign-on with LDAP
    - 190, 219

- SiteMinder (*continued*)
  - troubleshooting 191
  - Windows AD 219
- sites
  - access levels 89
- Solution Manager 403
- SPN utility 200
- SSL 116, 119, 120
  - certificates 117
  - configuring servers 116, 119, 120
  - configuring Web Application
    - Container Servers (WACS)
      - 351, 354
  - keys 117
  - report conversion tool 122
  - sslconfig.exe 121
  - thick clients 121
  - translation management tool 122
- SSL. See Secure Sockets Layer (SSL)
  - 180
- sslc.cnf 116
- sslc.exe 116
- statistics, auditing web activity 103
- status, viewing and changing for
  - servers 290, 291
- subgroups, adding 55
- Subversion 27
- syslog 308
- system account 228
- System Landscape Directory (SLD) 26
- system metrics, viewing 307
  - Web Application Container Server
    - (WACS) 367

**T**

- third-party security plug-ins 163
- tickets 100
  - for distributed security 100
  - logon tokens 99
- tiers 28
- Tomcat
  - JAAS 206
  - Kerberos 204
- top-level
  - folders, rights 81
- trace log
  - levels 461
- trace log level
  - CMC server setting 463
- tracing 461
  - servers 462
    - configuring .ini file 464
- tracking, sessions 100
- Traffic lights 403
- transfer of trust 100

- Trending Database 404
- Trending graph 403
- troubleshooting
  - Kerberos 225, 360
  - LDAP accounts 196
  - single sign-on 191
  - Web Application Container Servers
    - (WACS) 366
- troubleshooting network interfaces 318
- trust, active trust relationship 99
- trusted authentication
  - properties 172
    - sample configuration 176
- Trusted Authentication 169
  - SAML 171
    - user principal 178
- type-specific rights 76
  - access levels 487
  - Alerting 488
  - categories 484
  - CMC 487
  - folders 484
  - groups 486
  - notes 485
  - users 486

## U

- UNIX
  - syslog 308
- unmapping roles 247, 278
- Upgrade management tool 16, 37
- upgrades 28
- user accounts
  - creating 52
  - default 47
  - deleting 54
  - managing 47, 52
  - modifying 53
- user aliases 66
  - assigning 66
  - creating 66
    - for existing users 66
    - for new users 65
  - deleting 67
  - disabling 67
- user credentials, changing for nodes
  - 340
- users
  - assigning advanced rights to 80
  - assigning rights to 79
  - checking rights for 81, 82
  - granting access to 60
  - mapping 244, 261, 267, 273
  - rights 486
  - rights, on top-level folders 81

users (*continued*)  
 viewing rights for 79

## V

variables  
 installation directory 14, 321  
 node management scripts 321  
 script directory 14  
 UNIX operating system 14  
 version control 27  
 Version Management System settings  
 385  
 viewing  
 CMS cluster details 307  
 current metrics 307  
 rights for principals 79  
 system metrics 307  
 Web Application Container Server  
 (WACS) metrics 367  
 viewing current account 44, 288  
 Vintela 210  
 WebLogic considerations 214  
 virtual metrics 408

## W

WAR files  
 and Information platform services  
 web applications 151  
 BOE 152  
 dswsbobje 152  
 Information platform services web  
 applications 152  
 OpenDocument 210  
 Watch 403  
 WDeploy 38  
 Web Application Container Server  
 adding web services to 350  
 removing web services from 350

Web Application Container Server  
 (WACS) 22, 408, 492  
 AD Kerberos 360  
 adding 346  
 changing memory settings 368  
 cloning 349  
 CMC service 343  
 common tasks 344  
 connectors 343  
 creating new servers 348  
 deleting 349  
 firewalls 366  
 HTTPS 351, 354, 365  
 installing 347  
 JAAS files 358  
 Kerberos configuration files 358  
 load balancing 364  
 metrics 519  
 on multihomed computers 366  
 overview 343  
 properties 370  
 removing 346  
 resolving port conflicts 367, 368  
 restoring system defaults 369  
 server errors 367  
 SSL 351, 354  
 system metrics 367  
 troubleshooting 366  
 using with other web servers 364  
 using with proxy servers 365  
 web application servers 22  
 authentication 162  
 web clients 37  
 Web Intelligence 478  
 web servers  
 securing 102  
 web services  
 adding to a Web Application  
 Container Server 350  
 configuration for reverse proxy  
 servers 157  
 removing from a Web Application  
 Container Server 350

Web Services SDK and QaaWS  
 adding to a Web Application  
 Container Server 350  
 removing from a Web Application  
 Container Server 350  
 WebLogic  
 JAAS configuration file 206  
 Java options 209  
 Kerberos 204  
 WebSphere  
 JAAS 207  
 Java options 209  
 Kerberos 205  
 Windows  
 Event Log 308  
 server dependencies, adding 340  
 Windows AD  
 accounts and groups 198  
 scheduling updates 198  
 authentication 196  
 enabling Kerberos 356, 357  
 Kerberos configuration  
 application server 203  
 mapping LDAP 194  
 security plug-in 197  
 service account 211  
 single sign-on 211, 214  
 Vintela 214  
 workflows 39  
 access control lists, assigning  
 principals to 79  
 advanced rights, assigning 80  
 running a scheduled program  
 object 41  
 setting a schedule for a program  
 object 41  
 setting top-level folder rights 81  
 SIA shutdown 40  
 SIA start-up 39  
 user logon 39  
 viewing rights 79