SAP BusinessObjects Business Intelligence platform
Document Version: 4.1 Support Package 5 - 2015-01-09

Business Intelligence Platform Administrator Guide

Content

1 Document History. 19

2 Getting Started. 21

2.1 About this guide. 21

Who should use this guide?. 21

About the Business Intelligence platform. 21

Variables. 22

Terminology. 22

2.2 Before you start. 24

Key concepts. 24

Key administrative tools. 27

Key tasks. 28

3 Architecture. 31

3.1 Architecture overview. 31

Component diagram. 32

Architecture tiers. 33

Databases. 34

Servers, hosts, and clusters. 35

Web application servers. 35

Software Development Kits. 36

Data sources. 38

Authentication and single sign-on. 39

SAP integration. 40

Integrated version control. 41

Upgrade path. 41

3.2 Servers, services, nodes, and hosts. 42

Server changes since XI 3.1. 44

Services. 45

Service categories. 51

Server types. 53

Servers. 57

3.3 Client applications. 58

Installed with SAP BusinessObjects Business Intelligence platform Client Tools. 59

Installed with SAP BusinessObjects Business Intelligence platform. 63

Available separately. 64

Web application clients. 65

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.4 Process Workflows. 68
Startup and authentication. 68
Program objects. 70
Crystal Reports. 71
Web Intelligence. 75
Analysis. 77

4 System Configuration Wizard. 78
4.1 Introduction to the System Configuration Wizard. 78
4.2 Specifying the products you use. 78
4.3 Choosing a deployment template. 80
4.4 Specifying data folder locations. 82
4.5 Reviewing your changes. 83
4.6 Log files and response files. 83
Using a response file. 84

5 Managing Licenses. 88
5.1 Managing license keys. 88
To view license information. 88
To add a license key. 88
To view current account activity. 89

6 Managing Users and Groups. 90
6.1 Account management overview. 90
User management. 90
Group management. 90
Available authentication types 91
6.2 Managing Enterprise and general accounts. 93
To create a user account. 93
To modify a user account. 94
To delete a user account. 94
To create a new group. 95
To modify a group's properties. 95
To view group members. 96
To add subgroups. 96
To specify group membership. 97
To delete a group. 97
To add users or user groups in bulk. 98
To enable the Guest account. 98
Adding users to groups. 99
Changing password settings. 100
Granting access to users and groups. 101

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Controlling access to user inboxes. . . . 102
Configuring BI launch pad options. . . . 102
Managing attributes for system users 105
Prioritizing user attributes across multiple authentication options. . . . 106
To add a new user attribute. . . . 106
To edit customised user attributes. . . . 107
6.3 Managing aliases. . . . 108
To create a user and add a third-party alias. . . . 108
To create a new alias for an existing user. . . . 109
To assign an alias from another user. . . . 109
To delete an alias. . . . 110
To disable an alias. . . . 111

7 Setting Rights. . . . 112
7.1 How rights work in BI platform. . . . 112
Access levels. . . . 112
Advanced rights settings. . . . 113
Inheritance. . . . 114
Type-specific rights. . . . 118
Determining effective rights. . . . 120
7.2 Managing security settings for objects in the CMC. . . . 120
To view rights for a principal on an object. . . . 121
To assign principals to an access control list for an object. . . . 121
To modify security for a principal on an object. . . . 122
To set rights on a top-level folder in the BI platform. . . . 122
Checking security settings for a principal. . . . 123
7.3 Working with access levels. . . . 125
Choosing between *View* and *View On Demand* access levels. . . . 127
To copy an existing access level. . . . 128
To create a new access level. . . . 128
To rename an access level. . . . 128
To delete an access level. . . . 128
To modify rights in an access level. . . . 129
Tracing the relationship between access levels and objects. . . . 130
Managing access levels across sites. . . . 130
7.4 Breaking inheritance. . . . 132
To disable inheritance. . . . 133
7.5 Using rights to delegate administration. . . . 133
Choosing between "*Modify the rights users have to objects*" options. . . . 135
Owner rights. . . . 136
7.6 Summary of recommendations for rights administration. . . . 136

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8 Securing the BI Platform. 137
8.1 Security overview 137
8.2 Disaster recovery planning. 137
8.3 General recommendations for securing your deployment. 138
8.4 Configuring security for bundled third-party servers. 139
8.5 Active trust relationship. 139
Logon tokens. 139
Ticket mechanism for distributed security. 140
8.6 Sessions and session tracking. 140
CMS session tracking. 141
Managing sessions. 141
8.7 Environment protection. 142
Web browser to web server. 142
Web server to BI platform. 143
8.8 Auditing security configuration modifications 143
8.9 Auditing web activity. 143
Protection against malicious logon attempts. 143
Password restrictions. 144
Logon restrictions. 144
User restrictions. 144
Guest account restrictions. 145
8.10 Processing extensions. 145
8.11 Overview of BI platform data security. 145
Data processing security modes. 146
8.12 Cryptography in the BI platform. 148
Working with cluster keys. 148
Cryptographic Officers. 150
Managing cryptographic keys in the CMC. 152
8.13 Configuring servers for SSL. 156
Creating key and certificate files. 156
Setting up SSL when the certificate is managed by a certificate authority. 158
Configuring the SSL protocol. 160
8.14 Understanding communication between BI platform components. 165
Overview of BI platform servers and communication ports. 165
Communication between BI platform components 167
8.15 Configuring the BI platform for firewalls. 172
To configure the system for firewalls. 173
Debugging a firewalled deployment. 176
8.16 Examples of typical firewall scenarios. 177
Example - Application tier deployed on a separate network. 177
Example - Thick client and database tier separated from BI platform servers by a firewall. 179

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.17 Firewall settings for integrated environments. . . . 182
Specific firewall guidelines for SAP integration. . . . 182
Firewall configuration for JD Edwards EnterpriseOne integration. . . . 184
Specific firewall guidelines for Oracle EBS. . . . 185
Firewall configuration for PeopleSoft Enterprise integration . . . 186
Firewall configuration for Siebel integration. . . . 187
8.18 The BI platform and reverse proxy servers . . . 188
Supported reverse proxy servers . . . 188
Understanding how web applications are deployed . . . 189
8.19 Configuring reverse proxy servers for BI platform web applications. . . . 189
Detailed instructions for configuring reverse proxy servers. . . . 189
To configure the reverse proxy server. . . . 190
To configure Apache 2.2 reverse proxy server for the BI platform . . . 191
To configure WebSEAL 6.0 reverse proxy server for the BI platform . . . 191
To configure Microsoft ISA 2006 for the BI platform . . . 192
8.20 Special configuration for the BI platform in reverse proxy deployments. . . . 193
Enabling reverse proxy for web services. . . . 194
Enabling the root path for session cookies for ISA 2006. . . . 196
Enabling reverse proxy for SAP BusinessObjects Live Office. . . . 198

9 Authentication. . . . 199
9.1 Authentication options in the BI platform. . . . 199
Primary authentication. . . . 200
Security plug-ins. . . . 201
Single sign-on to the BI platform. . . . 201
9.2 Enterprise authentication. . . . 203
Enterprise authentication overview. . . . 203
Enterprise authentication settings. . . . 204
To change Enterprise settings. . . . 204
Enabling Trusted Authentication. . . . 206
Configuring Trusted Authentication for the web application. . . . 207
9.3 LDAP authentication. . . . 217
Using LDAP authentication. . . . 217
Configuring LDAP authentication. . . . 218
Mapping LDAP groups. . . . 228
9.4 Windows AD authentication. . . . 237
Using Windows AD authentication. . . . 237
Preparing the Domain Controller. . . . 238
Configuring AD Authentication in the CMC. . . . 239
Configuring the BI platform service to run the SIA. . . . 245
Configuring the web application server for AD Authentication. . . . 247
Single Sign-On Setup. . . . 256

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Troubleshooting Windows AD authentication. . . . 269
9.5 SAP authentication. . . . 271
Configuring SAP authentication . . . 271
Creating a user account for the BI platform. . . . 272
Connecting to SAP entitlement systems. . . . 273
Setting SAP Authentication options. . . . 275
Importing SAP roles. . . . 278
Configuring Secure Network Communication (SNC). . . . 282
Setting up single sign-on to the SAP system. . . . 294
Configuring SSO for SAP Crystal Reports and SAP NetWeaver. . . . 297
9.6 PeopleSoft authentication. . . . 299
Overview. . . . 299
Enabling PeopleSoft Enterprise authentication. . . . 299
Mapping PeopleSoft roles to the BI Platform. . . . 300
Scheduling user updates. . . . 302
Using the PeopleSoft Security Bridge. . . . 304
9.7 JD Edwards authentication. . . . 313
Overview. . . . 313
Enabling JD Edwards EnterpriseOne authentication. . . . 313
Mapping JD Edwards EnterpriseOne roles to the BI Platform. . . . 314
Scheduling user updates. . . . 316
9.8 Siebel authentication. . . . 318
Enabling Siebel authentication. . . . 318
Mapping roles to the BI platform. . . . 318
Scheduling user updates. . . . 321
9.9 Oracle EBS authentication. . . . 322
Enabling Oracle EBS authentication. . . . 322
Mapping Oracle E-Business Suite roles to the BI platform. . . . 323
Unmapping roles . . . 327
Customizing rights for mapped Oracle EBS groups and users . . . 327
Configuring Single Sign-on (SSO) for SAP Crystal Reports and Oracle EBS. . . . 328

10 Server Administration. . . . 330
10.1 Working with the Servers management area in the CMC. . . . 330
10.2 Managing servers by using scripts on Windows . . . 333
10.3 Managing servers on Unix . . . 333
10.4 Viewing and changing a server's status. . . . 333
Viewing the state of servers. . . . 333
Starting, stopping, and restarting servers. . . . 335
Stopping a Central Management Server. . . . 337
Enabling and disabling servers. . . . 338
10.5 Adding, cloning, or deleting servers. . . . 339

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Adding, cloning, and deleting servers. . . . 339
10.6 Clustering Central Management Servers. . . . 342
Clustering Central Management Servers. . . . 342
10.7 Managing server groups. . . . 347
Creating a server group. . . . 347
Working with server subgroups. . . . 348
Modifying the group membership of a server. . . . 349
Administrative access to servers and server groups for users. . . . 350
10.8 Configuring Adaptive Processing Servers for production systems. . . . 351
10.9 Assessing your system's performance. . . . 352
Monitoring BI platform servers. . . . 352
Analyzing server metrics. . . . 352
Viewing system metrics. . . . 353
Logging server activity. . . . 353
10.10 Configuring server settings. . . . 354
To change a server's properties. . . . 355
To apply service settings to multiple servers. . . . 355
Working with configuration templates. . . . 355
10.11 Configuring server network settings. . . . 358
Network environment options. . . . 358
Server host identification options. . . . 359
Configuring a multi-homed machine. . . . 360
Configuring port numbers. . . . 363
10.12 Managing Nodes. . . . 366
Using nodes. . . . 366
Adding a new node. . . . 368
Recreating a node. . . . 372
Deleting a node. . . . 375
Renaming a node. . . . 377
Moving a node. . . . 379
Script parameters. . . . 383
Adding Windows server dependencies. . . . 387
Changing the user credentials for a node. . . . 388
10.13 Renaming a machine in a BI platform deployment. . . . 389
Changing cluster names. . . . 389
Changing IP addresses. . . . 389
Renaming machines. . . . 391
10.14 Using 32-bit and 64-bit third-party libraries with BI platform. . . . 394
10.15 Managing server and node placeholders. . . . 395
To view server placeholders. . . . 395
To view and edit the placeholders for a node. . . . 395

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

11 Managing Central Management Server (CMS) Databases. 396
11.1 Managing CMS system database connections. 396
To select SQL Anywhere as a CMS database. 396
To select SAP HANA as a CMS database. 397
11.2 Selecting a new or existing CMS database. 398
To select a new or existing CMS database on Windows. 399
To select a new or existing CMS database on UNIX. 399
11.3 Recreating the CMS system database. 400
To recreate the CMS system database on Windows. 400
To recreate the CMS system database on UNIX. 401
11.4 Copying data from one CMS system database to another. 402
Preparing to copy a CMS system database. 403
To copy a CMS system database on Windows. 403
To copy data from a CMS system database on UNIX. 404

12 Managing Web Application Container Servers (WACS). 405
12.1 WACS. 405
Web Application Container Server (WACS). 405
Adding or removing additional WACS to your deployment. 407
Adding or removing services to WACS. 411
Configuring HTTPS/SSL. 412
Supported authentication methods. 415
Configuring AD Kerberos for WACS 415
Configuring AD Kerberos single sign-on 422
Configuring RESTful web services. 425
WACS and your IT environment. 434
Configuring web application properties. 436
Troubleshooting. 437
WACS properties. 440

13 Backing Up and Restoring Your System. 442
13.1 Overview of backup and restore. 442
13.2 Terminology. 442
13.3 Use cases for backup and restore. 443
13.4 Backups. 445
Backing up the entire system. 445
Backing up server settings. 448
Backing up BI content. 451
13.5 Restoring your system. 451
Restoring your entire system. 451
Restoring server settings. 456
Restoring BI content. 458

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13.6 BackupCluster and RestoreCluster scripts. . . . 459

14 Copying Your BI Platform Deployment. . . . 462
14.1 Overview of system copying. . . . 462
14.2 Terminology. . . . 462
14.3 Use cases for system copying. . . . 462
14.4 Planning to copy your system. . . . 463
14.5 Considerations and limitations. . . . 464
14.6 System copy procedure. . . . 466
To export from a source system. . . . 466
To import to a target system. . . . 470

15 Promotion Management. . . . 473
15.1 Welcome to promotion management. . . . 473
Overview. . . . 473
Features. . . . 473
Application access rights. . . . 474
Support for WinAD in promotion management. . . . 475
Override information in BI platform 4.1 SP3 and newer. . . . 475
To override connections between the Application Server and the Message Server. . . . 475
15.2 Getting started with the promotion management tool. . . . 476
Accessing the promotion management tool. . . . 476
User interface components. . . . 476
Using the Settings option. . . . 478
15.3 Using the promotion management tool. . . . 484
Creating and deleting folders. . . . 485
To create a job. . . . 486
To create a new job by copying an existing job 488
To search for a job. . . . 489
To edit a job. . . . 489
To add an infoobject to a job. . . . 490
To manage the dependencies of a job. . . . 491
To search for dependents 492
To promote a job when repositories are connected. . . . 492
Promoting a job using an LCMBIAR File. . . . 494
To schedule a job promotion. . . . 497
To view the history of a job. . . . 498
To roll back a job. . . . 499
15.4 To manage different versions of an infoobject. . . . 501
Version Management application access rights. . . . 502
Backing up and restoring Subversion files. . . . 502
15.5 Promoting full repository content using the promotion management tool. . . . 503

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

To prepare the source and target systems. . . . 503
Migration strategies. . . . 505
15.6 Full system promotion steps. . . . 506
To promote users and user groups (Job 1). . . . 506
To promote dependent objects (Job 2). . . . 507
To promote primary objects (Job 3). . . . 508
Post-promotion. . . . 509
15.7 Using the Command Line option. . . . 509
To run the command-line tool on Windows. . . . 509
To run the command-line tool on Unix. . . . 510
Command-line tool parameters. . . . 510
Sample properties file. . . . 516
15.8 Using the Enhanced Change and Transport System. . . . 517
Prerequisites. . . . 517
To configure the BI platform and CTS+ Integration. . . . 518
To promote a job using CTS. . . . 524

16 Version Management. . . . 528
16.1 To manage different versions of BI resources 528
16.2 Starting and stopping Subversion manually on Unix. . . . 529
16.3 Required files for Subversion on Solaris 10 and RedHat Linux 5. . . . 529
16.4 To use the Version Management System settings option. . . . 530
Default Version Management System settings. . . . 531
To set the ClearCase Version Management System in Windows. . . . 531
To set the ClearCase Version Management System in Unix. . . . 532
16.5 To compare different versions of the same job. . . . 532
16.6 To upgrade Subversion content. . . . 533
16.7 Configuring Subversion for clustered Processing Job Servers. . . . 533
Option A: To configure the main Subversion machine before any Version Management System operations. . . . 533
Option B: To configure Subversion after the Version Management System creates a working copy directory. . . . 534
Configuring other Subversion machines. . . . 535
16.8 To access the same ClearCase view from multiple Version Management Servers. . . . 535

17 Visual Difference. . . . 537
17.1 Visual Difference in the promotion management tool. . . . 537
To compare objects or files using Visual Difference. . . . 538
To compare objects or files using the Version Management System. . . . 539
To schedule the comparison. . . . 540

18 Managing Applications. . . . 541
18.1 Managing applications through the CMC. . . . 541

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Overview. . . . 541
Common settings for applications. . . . 542
Application-specific settings. . . . 543
18.2 Managing applications through BOE.war properties. . . . 579
The BOE war file. . . . 579
18.3 Customizing BI launch pad and OpenDocument logon entry points. . . . 587
BI launch pad and OpenDocument file locations. . . . 588
To define a custom logon page. . . . 588
To add trusted authentication at logon. . . . 589
18.4 Customizing application user interfaces. . . . 590
Web Intelligence. . . . 590
BI launch pad. . . . 604

19 Managing Connections and Universes. . . . 605
19.1 Managing connections. . . . 605
To delete a universe connection. . . . 605
19.2 Managing universes. . . . 606
To delete universes. . . . 606

20 Monitoring. . . . 607
20.1 About Monitoring. . . . 607
20.2 Monitoring terms. . . . 607
Architecture. . . . 609
20.3 Configuring database support for Monitoring 611
Configuration for using the Derby database. . . . 612
Configuration for using the auditing database. . . . 612
20.4 Configuration properties. . . . 619
JMX end point URL. . . . 621
HTTPS authentication for monitoring probes. . . . 622
Password encryption for probes. . . . 623
20.5 Integrating with other applications. . . . 623
Integrating the monitoring application with IBM Tivoli. . . . 623
Integrating the monitoring application with SAP Solution Manager 626
20.6 Cluster support for monitoring server. . . . 626
20.7 Troubleshooting. . . . 627
Dashboard. . . . 627
Alerts. . . . 627
Watchlist. . . . 628
Probes. . . . 629
Metrics. . . . 629
Graph. . . . 630

21 Auditing. . . . 631

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

21.1 Overview. . . . 631
21.2 CMC Auditing page. . . . 637
Auditing Status. . . . 637
Configuring Auditing events. . . . 639
Auditing Data Store configuration settings. . . . 641
21.3 Audit events. . . . 643
Audit events and details. . . . 651

22 Platform Search. . . . 669
22.1 Understanding Platform Search. . . . 669
Platform Search SDK. . . . 669
Clustered Environment. . . . 669
22.2 Setting Up Platform Search. . . . 670
Deploying OpenSearch. . . . 670
Configuring reverse proxy. . . . 671
Configuring Application Properties in the CMC. . . . 672
22.3 Working with Platform Search. . . . 676
Indexing Content in the CMS Repository. . . . 676
Indexing Failure Listing. . . . 677
Searching Results. . . . 678
22.4 Integrating Platform Search with SAP NetWeaver Enterprise Search. . . . 684
Creating a Connector in SAP NetWeaver Enterprise Search 684
Importing a User's Role into the BI platform. . . . 685
22.5 Searching from SAP NetWeaver Enterprise Search. . . . 685
22.6 Auditing. . . . 686
22.7 Troubleshooting. . . . 687
Self Healing. . . . 687
Problem Scenarios. . . . 687

23 Federation. . . . 690
23.1 Federation. . . . 690
23.2 Federation terms. . . . 691
23.3 Managing security rights. . . . 692
Rights required on the origin site. . . . 693
Rights required on the destination site. . . . 693
Federation-specific rights. . . . 694
Replicating security on an object. . . . 695
Replicating security using access levels. . . . 696
23.4 Replication types and mode options. . . . 696
One-way replication 696
Two-way replication 697
Refresh from origin or refresh from destination. . . . 697

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.5 Replicating third-party users and groups. . . . 698
23.6 Replicating universes and universe connections. . . . 699
23.7 Managing replication lists. . . . 700
Creating replication lists. . . . 701
Modifying Replication Lists. . . . 703
23.8 Managing remote connections. . . . 704
Creating remote connections. . . . 704
Modifying remote connections. . . . 706
23.9 Managing replication jobs. . . . 707
Creating replication jobs. . . . 707
Scheduling replication jobs. . . . 709
Modifying replication jobs. . . . 709
Viewing a log after a replication job. . . . 710
23.10 Managing object cleanup. . . . 711
How to use object cleanup. . . . 711
Object cleanup limits. . . . 711
Object cleanup frequency. . . . 712
23.11 Managing conflict detection and resolution. . . . 713
One-way replication conflict resolution. . . . 713
Two-way replication conflict resolution. . . . 715
23.12 Using Web Services in Federation. . . . 718
Session variables 718
File caching 719
Custom deployment 719
23.13 Remote scheduling and locally run instances. . . . 720
Remote scheduling. . . . 720
Locally run instances. . . . 721
Instance share. . . . 722
23.14 Importing and promoting replicated content. . . . 723
Importing replicated content. . . . 723
Importing replicated content and continuing replication 723
Promoting content from a test environment. . . . 724
Re-pointing a destination site. . . . 725
23.15 Best practices. . . . 725
Current release limitations. . . . 728
Troubleshooting error messages. . . . 729

24 Supplementary Configurations for ERP Environments. . . . 733
24.1 Configurations for SAP NetWeaver integration. . . . 733
Integrating with SAP Business Warehouse (BW). . . . 733
24.2 Configuring for JD Edwards integration. . . . 774
Configuring Single Sign-on (SSO) for SAP Crystal Reports. . . . 774

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Configuring Secure Sockets Layer for JD Edwards Integrations. 775
24.3 Configuring for PeopleSoft Enterprise integration. 776
Configuring Single Sign-on (SSO) for SAP Crystal Reports and PeopleSoft Enterprise. 776
Configuring Secure Sockets Layer communication. 777
Performance Tuning for PeopleSoft systems. 779
24.4 Configuring for Siebel integration. 780
Configuring Siebel to integrate with SAP BI platform. 780
Creating the Crystal Reports menu item. 781
Contextual awareness. 782
Configuring Single Sign-on (SSO) for SAP Crystal Reports and Siebel. 784
Configuring for Secure Sockets Layer Communication. 785

25 Managing and Configuring Logs. 787
25.1 Logging traces for components. 787
25.2 Trace log levels. 787
25.3 Configuring tracing for servers. 788
To set the log level in the CMC. 788
To set the log level for multiple servers in the CMC. 789
To configure server tracing using the BO_trace.ini file. 789
25.4 Configuring tracing for web applications. 791
To set the web application trace log level in the CMC. 792
To configure tracing settings using the `BO_trace.ini` file. 793
25.5 Configuring tracing for upgrade management tool. 797
To configure tracing for upgrade management tool. 797
25.6 Configuring tracing for BI platform client applications. 798

26 Integration to SAP Solution Manager. 799
26.1 Integration overview. 799
26.2 SAP Solution Manager integration checklist. 799
26.3 Managing system landscape directory registration. 800
Registration of the BI platform in the System Landscape. 800
When is SLD registration triggered?. 801
Logging SLD connectivity 802
26.4 Managing Solution Management Diagnostics agents. 802
Solution Manager Diagnostics (SMD) overview. 802
Working with SMD agents. 802
SMAdmin user account. 803
26.5 Managing performance instrumentation. 804
Performance instrumentation for the BI platform. 804
Setting up performance instrumentation for the BI platform. 804
Performance instrumentation for the web tier. 805
Instrumentation log files 805

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

26.6 Tracing with SAP Passport. . . . 806

27 Command Line Administration. . . . 807

27.1 Unix scripts. . . . 807

Script utilities. . . . 807

Script templates. . . . 812

Scripts used by the BI platform. . . . 812

27.2 Windows scripts. . . . 814

ccm.exe. . . . 814

27.3 Server Command Lines. . . . 817

Command lines overview. . . . 817

Standard options for all servers. . . . 817

Central Management Server. . . . 818

Crystal Reports Processing Server and Crystal Reports Cache Server. . . . 820

Dashboards Processing Server and Dashboards Cache Server. . . . 821

Job Servers. . . . 822

Adaptive Processing Server. . . . 822

Report Application Server. . . . 823

Web Intelligence Processing Server. . . . 824

Input and Output File Repository Servers. . . . 826

Event Server. . . . 827

28 Repository Diagnostic Tool. . . . 829

28.1 Overview of the Repository Diagnostic Tool. . . . 829

28.2 Using the Repository Diagnostic Tool. . . . 829

To use the Repository Diagnostic Tool. . . . 830

Repository Diagnostic Tool Parameters. . . . 831

28.3 Inconsistencies between the CMS and the FRS. . . . 836

28.4 Inconsistencies in the CMS metadata. . . . 837

29 Rights Appendix. . . . 840

29.1 About the rights appendix. . . . 840

29.2 General rights. . . . 840

29.3 Rights for specific object types. . . . 842

Folder rights. . . . 842

Categories. . . . 843

Desktop Intelligence documents. . . . 843

Notes. . . . 845

Crystal reports. . . . 845

Web Intelligence documents. . . . 845

Users and groups. . . . 846

Access levels. . . . 847

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Universe (.unv) rights. . . . 848
Universe (.unx) rights. . . . 849
Universe object-access levels. . . . 851
Connection rights. . . . 852
Applications. . . . 853

30 Server Properties Appendix. . . . 867
30.1 About the server properties appendix. . . . 867
Common Server Properties. . . . 867
Core Services properties. . . . 869
Connectivity Services Properties. . . . 879
Crystal Reports Services Properties. . . . 883
Analysis Services Properties. . . . 891
Data Federation Services Properties. . . . 892
Web Intelligence Services properties. . . . 893
Dashboards Services Properties. . . . 899

31 Server Metrics Appendix. . . . 902
31.1 About the Server Metrics Appendix. . . . 902
Common Server Metrics 903
Central Management Server Metrics. . . . 904
Connection Server Metrics. . . . 907
Event Server Metrics. . . . 908
File Repository Server Metrics. . . . 908
Adaptive Processing Server Metrics. . . . 909
Web Application Container Server Metrics. . . . 913
Adaptive Job Server Metrics. . . . 913
Crystal Reports Server Metrics. . . . 915
Web Intelligence Server Metrics. . . . 917
Dashboards Server Metrics. . . . 918

32 Server and Node Placeholder Appendix. . . . 921
32.1 Server and node placeholders. . . . 921

33 Auditing Data Store Schema Appendix. . . . 929
33.1 Overview. . . . 929
33.2 Schema diagram. . . . 929
33.3 Auditing Data Store Tables. . . . 929

34 Monitoring Database Schema Appendix. . . . 937
34.1 Trending database schema. . . . 937

35 System Copy Worksheet Appendix. . . . 940

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

35.1 System copy worksheet. 940

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1 Document History

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

Table 1:

Version	Date	Description
SAP BusinessObjects BI platform 4.1	May 2013	First release of this document.
SAP BusinessObjects BI platform 4.1 Support Package 1	August 2013	• The "Promotion Management" chapter is updated. • The "Managing Licenses" chapter is updated. • Other corrections and minor updates.

SAP BusinessObjects BI platform 4.1 Support Package 2	November 2013	• The "Version Management" chapter is updated.
		  ○ The "To launch Version Management on Solaris 10" section has been added.
		  ○ The "Starting and stopping Subversion manually on Unix" section has been added.
		  ○ The "Default Version Management system settings" section has been added.
		  ○ The "To use the Version Management System settings option" section has been updated.
		• The "Promotion Management" chapter is updated.
		  ○ The "Using LCM Override Settings option" section has been updated.
		  ○ The "Using the Command Line option" section has been updated.
		  ○ The "Command-line tool parameters" section has been updated.
		• The "Repository Diagnostic Tool" chapter is updated.
		• The "Customizing the Web Intelligence interface" section is updated.
		• Other corrections and minor updates.

SAP BusinessObjects BI platform 4.1 Support Package 3	March 2014	• Added the "Managing sessions" section. • Reorganized and updated the "Customizing application user interfaces" section. • Added Design Studio auditing. • Added section describing how to change the CMS request port. • Added information on using Oracle databases for monitoring.
SAP BusinessObjects BI platform 4.1 Support Package 4	June 2014	• Added BI launch pad to the "Managing Applications" section. • Added a `-legacymode` command-line parameter for the File Repository Server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Version	Date	Description
SAP BusinessObjects BI platform 4.1 Support Package 5	November 2014	• Added the SAP Lumira section under "Architecture > Client Applications > Available Separately". • Added SAP Lumira to the “Managing Applications > Managing applications through the CMC > Overview” section. • Added the "Managing SAP Lumira Settings" section under "Managing Applications > Managing applications through the CMC > Application-specific settings". • Updated the "Customization application user interfaces" section with folder customization feature. • Added Analysis Office and Lumira document types in the "Content Types" and "Searchable Content Types" sections. • Added a note on full content indexing support in the "Configuring Application Properties in the CMC" section. • Added a note on metadata search in the "Facets" section. • Updated the "Configuring SBO files" section. • Updated the default value for `-maxobjectsincache` option in the “Central management Server” section. • Updated the "Web Intelligence Services properties" section with **`-Dsap.sl.bics.variableComplexSelectionMapping=n`** command-line parameter. • Updated the "Repository Diagnostic Tool Parameters" section with the -trace command-line parameter. • Updated the maximum value for *Delete Events Older Than (Days)* field in the "To configure your Auditing Data Store database settings" section.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2 Getting Started

2.1 About this guide

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

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

2.1.1 Who should use this guide?

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

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

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

2.1.2 About the Business Intelligence platform

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

An integrated suite for reporting, analysis, and information delivery, the platform provides a solution for increasing end-user productivity and reducing administrative efforts. Whether it is used to distribute weekly sales reports, to provide customers with personalized service offerings, or to integrate critical information in corporate portals, the platform delivers tangible benefits that extend across and beyond the organization.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2.1.3 Variables

The following variables are used throughout this guide.

Variable	Description
<INSTALLDIR>	The directory where the BI platform is installed. On Windows, the default directory is `C:\Program Files (x86)\SAP BusinessObjects\`.
<PLATFORM64DIR>	The name of your Unix operating system. Acceptable values are: • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
<SCRIPTDIR>	The directory where scripts for administering the BI platform are located. On Windows, the directory is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`. On Unix, the directory is **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/`**<PLATFORM64DIR>**`/scripts`.

2.1.4 Terminology

The following terms are used throughout the BI platform documentation:

Table 2:

Term	Definition
add-on products	Products that work with the BI platform but have their own installation program, such as SAP BusinessObjects Explorer
Auditing Data Store (ADS)	The database used to store auditing data
BI platform	An abbreviation for the SAP BusinessObjects Business Intelligence platform
bundled database; bundled web application server	The database or web application server shipped with the BI platform
cluster (noun)	Two or more Central Management Servers (CMSs) working together and using a single CMS database

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Term	Definition
cluster (verb)	To create a cluster. For example, to create a cluster: 1. Install a CMS and CMS database on machine A. 2. Install a CMS on machine B. 3. Point the CMS on machine B to the CMS database on machine A.
cluster key	Used to decrypt the keys in the CMS database. You can change the cluster key in the CCM, but you cannot reset the key like a password. It contains encrypted content and is important not to lose.
CMS	An abbreviation for the Central Management Server
CMS database	The database used by the CMS to store information about the BI platform
deployment	The BI platform software installed, configured, and running on one or more machines
installation	An instance of BI platform files created by the installation program on a machine
machine	The computer on which the BI platform software is installed
major release	A full release of the software, such as 4.0
migration	The process of transferring BI content from a previous major release (for example, from XI 3.1), using the upgrade management tool. This term does not apply to deployments with the same major release. See *promotion*.
minor release	A release of some components of the software, such as 4.1
node	A group of BI platform servers that run on the same machine and are managed by the same Server Intelligence Agent (SIA)
Patch	A small update for a specific Support Package version
promotion	The process of transferring BI content between deployments with the same major release (for example, 4.0 to 4.0), using the promotion management application
server	A BI platform process. A server hosts one or more services.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Term	Definition
Server Intelligence Agent (SIA)	A process that manages a group of servers, including stopping, starting, and restarting servers
Support Package	A software update for a minor or major release
web application server	A server that processes dynamic content. For example, the bundled web application server for 4.1 is Tomcat 7.
upgrade	The planning, preparation, migration, and post-processes required to complete a migration process

2.2 Before you start

2.2.1 Key concepts

2.2.1.1 Server Intelligence

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Servers, hosts, and clusters [page 35]

2.2.1.2 Servers, services, nodes, and hosts

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

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

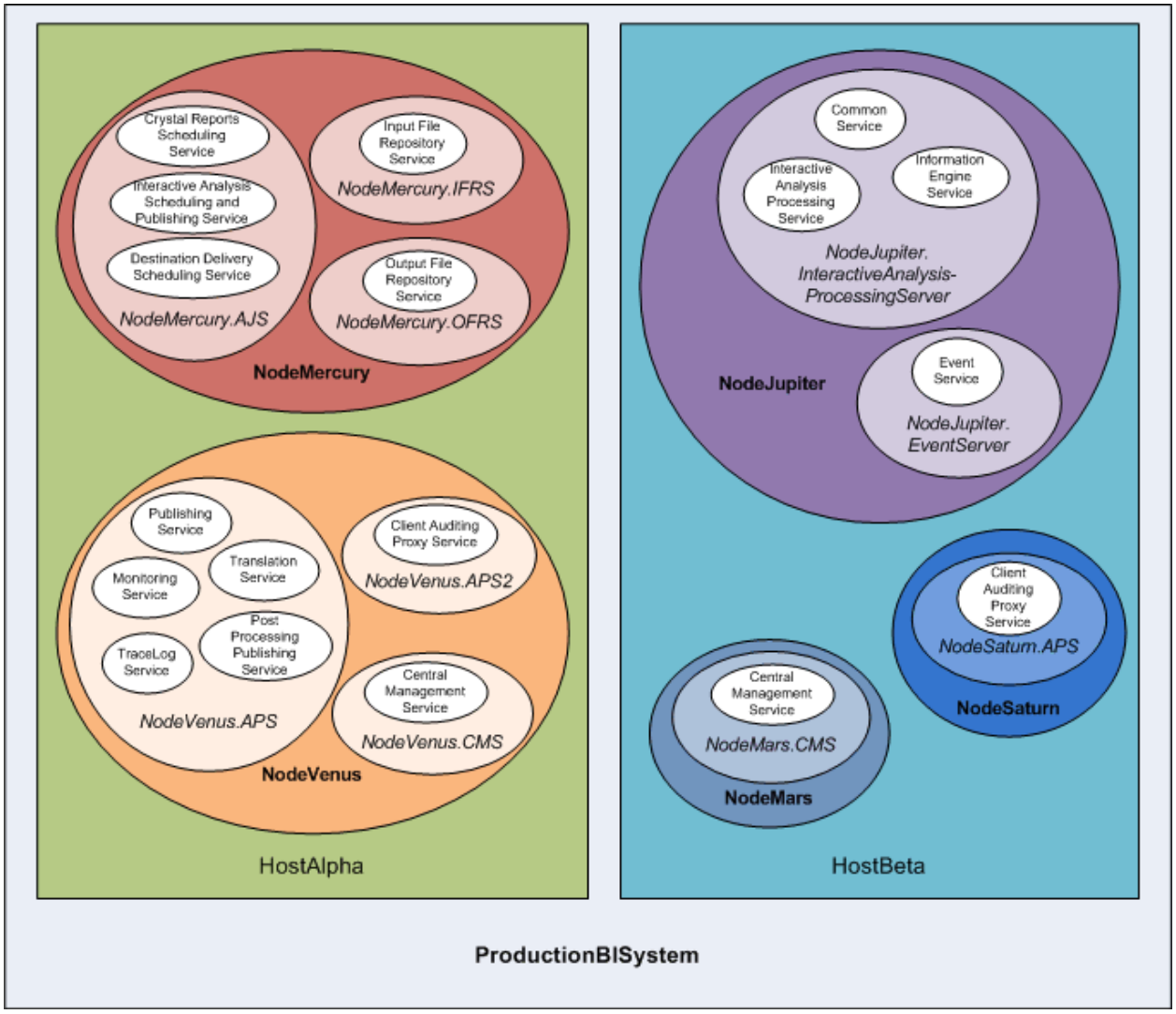
A service is a server subsystem that performs a specific function. The service runs within the memory space of its server under the process ID of the parent container (server). For example, the Web Intelligence Scheduling Service is a subsystem that runs within the Adaptive Job Server.

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.



Two hosts form the cluster named ProductionBISystem:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

2.2.2 Key administrative tools

2.2.2.1 System Configuration Wizard

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

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

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

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

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

2.2.2.2 Central Management Console (CMC)

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2.2.2.3 Central Configuration Manager (CCM)

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

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

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

2.2.2.4 Repository Diagnostic Tool

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

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

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

2.2.2.5 Upgrade management tool

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

For information on upgrading from a previous version of the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Upgrade Guide*.

2.2.3 Key tasks

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Planning or performing your first deployment [page 29]
Configuring your deployment [page 29]
Improving your system's performance [page 30]
Central Management Console (CMC) [page 27]

2.2.3.1 Planning or performing your first deployment

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

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

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

Related Information

Architecture overview [page 31]
Communication between BI platform components [page 167]
Security overview [page 137]
Authentication options in the BI platform [page 199]
Working with the Servers management area in the CMC [page 330]

2.2.3.2 Configuring your deployment

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

Related Information

Introduction to the System Configuration Wizard [page 78]
Communication between BI platform components [page 167]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Security overview [page 137]
About Monitoring [page 607]

2.2.3.3 Improving your system's performance

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

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

Related Information

Introduction to the System Configuration Wizard [page 78]
About Monitoring [page 607]
Working with the Servers management area in the CMC [page 330]

2.2.3.4 Working with objects in the CMC

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

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

Related Information

Account management overview [page 90]
How rights work in BI platform [page 112]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3 Architecture

3.1 Architecture overview

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

> **Note**
>
> For a list of supported platforms, languages, databases, web application servers, web servers, and other systems supported by this release, see the *Product Availability Matrix* (PAM) at the "Supported Platforms/PARs" link, available on the SAP Support Portal: http://service.sap.com/bosap-support.

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

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

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

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

- Clients installed by the BI platform Client Tools installation program:
  - Web Intelligence Rich Client
  - Business View Manager
  - Report Conversion Tool
  - Universe Design Tool
  - Query as a Web Service
  - Information Design Tool (formerly Information Designer)
  - Translation Management Tool (formerly Translation Manager)
  - Widgets (formerly BI Widgets)
- Clients available separately:
  - SAP Crystal Reports
  - SAP BusinessObjects Dashboards (formerly Xcelsius)
  - SAP BusinessObjects Analysis (formerly Voyager)
  - BI Workspaces (formerly Dashboard Builder)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

- Report viewers
- Central Management Console (CMC)
- Central Configuration Manager (CCM)
- Repository Diagnostic Tool (RDT)
- Data Federation Administration Tool
- Upgrade management tool (formerly a function within the Import Wizard)
- Universe Design Tool (formerly Universe Designer)
- SAP BusinessObjects Mobile

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

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

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

3.1.1 Component diagram

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

This architecture diagram, on the SAP Community Network, illustrates the BI platform components, including servers and client tools, and additional analytic products, web application components, and databases that can be part of a BI platform landscape: http://scn.sap.com/docs/DOC-43663.

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.1.2 Architecture tiers

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

Client tier

The client tier contains all desktop client applications that interact with the BI platform to provide a variety of reporting, analytic, and administrative capabilities. Examples include the Central Configuration Manager (BI platform installation program), Information design tool (BI platform Client Tools installation program), and SAP Crystal Reports (available and installed separately).

Web tier

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

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

Management tier

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

Storage tier

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

Processing tier

The processing tier analyzes data, and produces reports and other output types. This is the only tier that accesses the databases that contain report data. This tier comprises the Adaptive Job Server, Connection Server (32- and 64-bit), and processing servers such as the Adaptive Processing Server or Crystal Reports Processing Server.

Data tier

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

3.1.3 Databases

The BI platform uses several different databases.

- Reporting database
  This refers to your organization's data. It is the source data analyzed and reported on by SAP BusinessObjects Business Intelligence Suite products. Most commonly, the data is stored within a relational database, but it can also be contained within text files, Microsoft Office documents, or OLAP systems.
- CMS system database
  The CMS system database is used to store BI platform information, such as user, server, folder, document, configuration, and authentication details. It is maintained by the Central Management Server (CMS), and is sometimes referred to as the *system repository*.
- Auditing Data Store
  The Auditing Data Store (ADS) is used to store information on trackable events that occur in the BI platform. This information can be used to monitor the usage of system components, user activity, or other aspects of day-to-day operation.
- Lifecycle Management database
  The Lifecycle Management database tracks configuration and version information related to a BI platform 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 BI platform installation program can install and configure one for you. It is recommended that you evaluate your requirements against information from your database server vendor to determine which supported database would best suit your organization's requirements.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The default SQL Anywhere database is not recommended for production systems.

3.1.4 Servers, hosts, and clusters

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

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

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

3.1.5 Web application servers

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.1.5.1 Web Application Container Server (WACS)

A web application server is required to host BI platform 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 BI platform web applications. If you are using a supported Windows operating system to host the BI platform, 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 Server (WACS) when installing the BI platform.

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

Using WACS provides a number of advantages:

- WACS requires a minimum effort to install, maintain, and configure. It is installed and configured by the BI platform 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 BI platform servers.
- Like other BI platform servers, WACS can be installed on a dedicated host.

> **Note**
>
> There are some limitations to using WACS instead of a dedicated Java web application 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 the BI platform.
> - 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 BI platform web applications are hosted by WACS.

3.1.6 Software Development Kits

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

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

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

The following SDKs are supported by the BI platform:

- Business Intelligence platform Java SDK and .NET SDK

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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

- Data Access Driver and Connection Java SDKs
  These SDKs allow you to create database drivers for the Connection Server and manage database connections.
- Semantic Layer Java SDK
  The Semantic Layer Java SDK allows you to develop a Java application that performs administration and security tasks on universes and connections. For example, you can implement services for publishing a universe to a repository or retrieving a secured connection from the repository to your workspace. This application can be embedded within BI platform solutions that integrate the BI platform as OEM.
- Report Application Server Java SDK and .NET SDK
  The Report Application Server SDKs allow applications to open, create, and modify existing Crystal reports, including setting parameter values, changing data sources, and exporting to other formats, including XML, PDF, Microsoft Word, and Microsoft Excel.
- Java and .NET Crystal Reports Viewers
  The viewers allow applications to display and export Crystal reports. The following viewers are available:
  - DHTML Report Page Viewer: presents data and allows drill-down, page navigation, zooming, prompting, search, highlighting, exporting, and printing.
  - Report Parts Viewer: provides the ability to view individual parts of a report, including charts, text, and fields.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Report Engine Java SDK and .NET SDK
  The Report Engine SDKs allow applications to interact with reports created with SAP BusinessObjects Web Intelligence.
  The Report Engine SDKs include libraries that you can use to build a web report design tool. Applications built with these SDKs can view, create, or modify, a variety of different Web Intelligence documents. Users can modify documents by adding, removing, and modifying objects such as tables, charts, conditions, and filters.
- Platform Search SDK: The Platform Search SDK is the interface between the client application and the Platform Search Service. Platform Search supports Public SDK that comes as a part of the Platform Search SDK.
  When a search request parameter is sent through the client application to the SDK layer, the SDK layer converts the request parameter into XML- encoded format and passes it to the Platform Search Service.

The SDKs can be used in combination to provide a wide range of BI functionality to your applications. For more information on these SDKs, including developer guides and API references, see http://help.sap.com.

3.1.7 Data sources

3.1.7.1 Universes

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

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

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

3.1.7.2 Business Views

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.1.8 Authentication and single sign-on

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

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

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

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

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

3.1.8.1 Security plug-ins

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

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

The BI platform supports the following security plug-ins:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Windows AD

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

3.1.8.2 Enterprise Resource Planning (ERP) integration

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

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

> **Note**
>
> - SAP ERP and BW support is installed by default. Use the *Custom / Expand* installation option to deselect SAP integration support if you do not want support for SAP ERP or BW.
> - Support for Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne, or PeopleSoft is not installed by default. Use the *Custom / Expand* installation option to select and install integration for non-SAP ERP systems.

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

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

3.1.9 SAP integration

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- SAP Solution Manager
  The SAP Solution Manager is a platform that provides the integrated content, tools, and methodologies to implement, support, operate and monitor an organization's SAP and non-SAP solutions.
  Non-SAP software with an SAP-certified integration is entered into a central repository and transferred automatically to your SAP System Landscape Directories (SLD). SAP customers can then easily identify which version of third-party product integration has been certified by SAP within their SAP system environment. This service provides additional awareness for third-party products besides our online catalogs for third-party products.
  SAP Solution Manager is available to SAP customers at no extra charge, and includes direct access to SAP support and SAP product upgrade path information. For more information on SLD, see "Registration of the BI platform in the System Landscape".
- Change and Transport System (CTS+)
  The 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, JCOs, Classes, Methods and more. It offers real-time, low-overhead monitoring, end-to-end transaction visibility, historical data for analysis or capacity planning, customizable dashboards, automated threshold alarms, and an open architecture to extend monitoring beyond NetWeaver environments.

3.1.10 Integrated version control

The files that make up the BI platform on a server system are 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.

3.1.11 Upgrade path

It's possible to upgrade from a previous release of SAP BusinessObjects Enterprise (for example XI 3.x), but you must first install SAP BusinessObjects Business Intelligence platform 4.x, 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 *SAP BusinessObjects Business Intelligence Platform Upgrade Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.2 Servers, services, nodes, and hosts

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

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

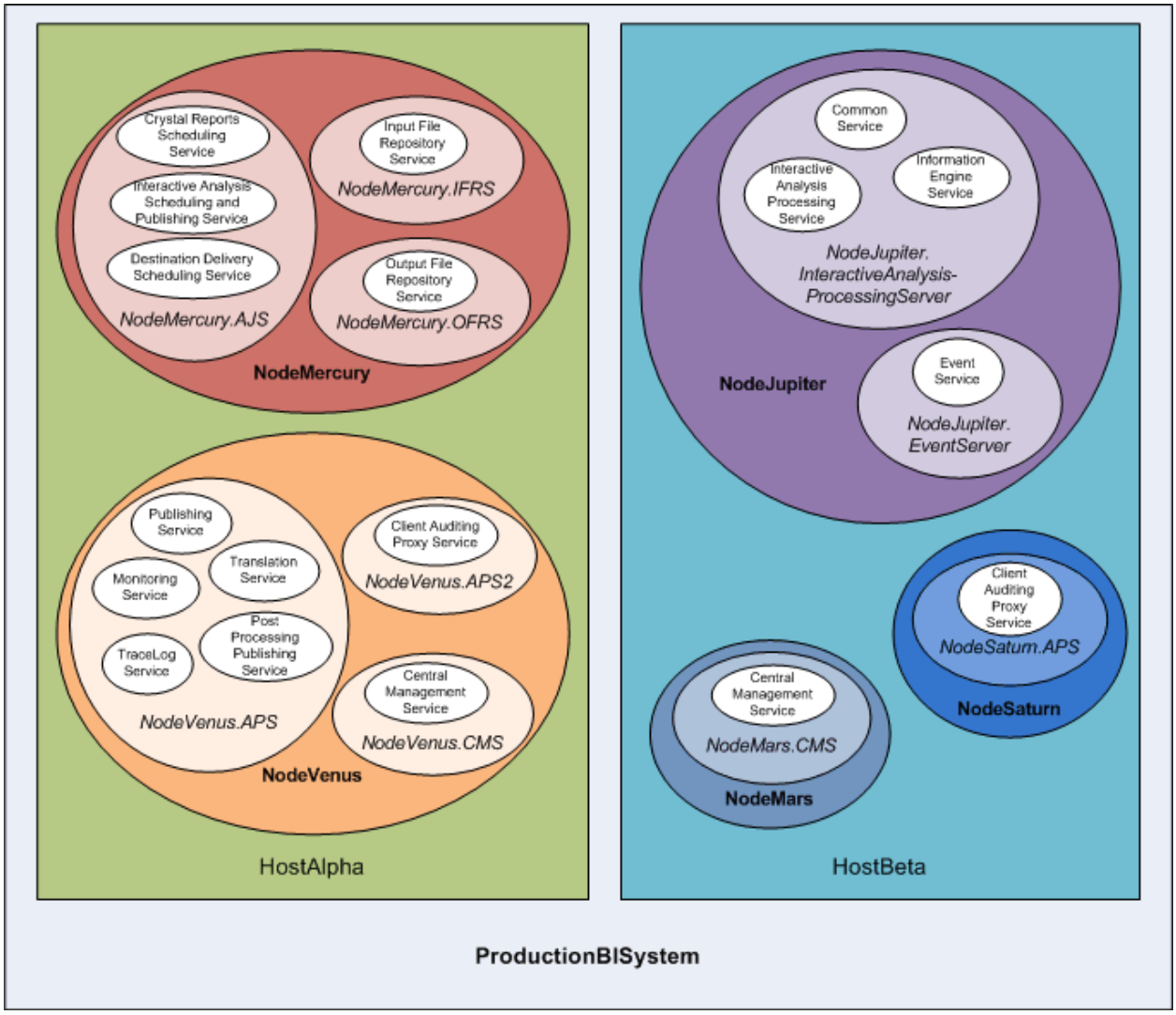
A service is a server subsystem that performs a specific function. The service runs within the memory space of its server under the process ID of the parent container (server). For example, the Web Intelligence Scheduling Service is a subsystem that runs within the Adaptive Job Server.

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.



Two hosts form the cluster named ProductionBISystem:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

3.2.1 Server changes since XI 3.1

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

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

Table 3: Server changes

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Connection Server [1]	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32
Crystal Reports Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Crystal Reports Processing Server	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)	Crystal Reports 2013 Processing Server Crystal Reports Processing Server (for SAP Crystal Reports for Enterprise reports)
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (BI Workspaces)	Not available as of 4.0 Feature Pack 3	Not available in 4.1
Dashboard Analytics Server (Dashboard Builder) [2]	Dashboard Analytics Server (BI Workspaces)	Not available as of 4.0 Feature Pack 3	Not available in 4.1
Desktop Intelligence Cache Server [3]	Not available as of 4.0	Not available as of 4.0	Not available in 4.1 [3]
Desktop Intelligence Job Server [3]	Not available as of 4.0	Not available as of 4.0	Not available in 4.1 [3]
Desktop Intelligence Processing Server [3]	Not available as of 4.0	Not available as of 4.0	Not available in 4.1 [3]
Destination Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
List of Values Server (LOV)	Web Intelligence Processing Server	Web Intelligence Processing Server	Web Intelligence Processing Server

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Multi-Dimensional Analysis Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server
Program Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2013 Report Application Server (RAS)
Web Intelligence Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Xcelsius Cache Server [4]	Dashboard Design Cache Server (Xcelsius) [5]	Dashboards Cache Server (Xcelsius)	Dashboards Cache Server (Xcelsius)
Xcelsius Processing Server [4]	Dashboard Design Processing Server (Xcelsius) [5]	Dashboards Processing Server (Xcelsius)	Dashboards Processing Server (Xcelsius)

- [1] In 4.0, Connection Server 32 is 32-bit and runs connections specifically to data sources that do not support 64-bit middleware. Connection Server is 64-bit and runs connections to all other data sources. For more information, see the *Data Access Guide*.
- [2] The Dashboard Server and Dashboard Analytics Server have been removed in 4.0 Feature Pack 3. Server configuration is no longer required for BI workspace functionality (formerly Dashboard Builder in XI 3.1).
- [3] Desktop Intelligence was not available in version 4.0 and 4.0 maintenance packs. The Desktop Intelligence client application is available in version 4.1, but Desktop Intelligence servers are not. Desktop Intelligence reports can be converted to Web Intelligence documents using the Report Conversion Tool.
- [4] The Xcelsius Cache and Processing Services were introduced as of XI 3.1 Service Pack 3 to optimize Query as a Web Service requests on relational data sources from Xcelsius. Equivalent Cache and Processing services are available on the Dashboards Cache Server and Dashboards Processing Server introduced in 4.0 Feature Pack 3.
- [5] Dashboard Design servers in 4.0 have been renamed to "Dashboards" in 4.0 Feature Pack 3 to align with the product name change to SAP BusinessObjects Dashboards.

3.2.2 Services

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

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

Table 4:

Service	Service category	Server type	Service description
Adaptive Connectivity Service	Connectivity Services	Adaptive Processing Server	Provides connectivity services for Java-based drivers

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service	Service category	Server type	Service description
Authentication Update Scheduling Service	Core Services	Adaptive Job Server	Provides synchronization of updates for third-party security plug-ins
BEx Web Application Service	Analysis Services	Adaptive Processing Server	Provides integration of SAP Business Warehouse (BW) Business Explorer (BEx) web applications with BI launch pad
BOE Web Application Service	Core Services	Web Application Container Server	Provides web applications for WACS, including the Central Management Console (CMC), BI launch pad, and OpenDocument
Business Process BI Service	Core Services	Web Application Container Server	Provides Business Process BI Web Services for WACS, allowing BI technology to be incorporated in web applications. Business Process BI Service is deprecated.
Central Management Service	Core Services	Central Management Server	Provides server, user, session management, and security (access rights and authentication) management. At least one Central Management Service must be available in a cluster for the cluster to operate.
Client Auditing Proxy Service	Core Services	Adaptive Processing Server	Collects auditing events sent from clients and forwards them to the CMS server
Crystal Reports 2013 Processing Service	Crystal Reports Services	Crystal Reports Processing Server	Accepts and processes Crystal Reports 2013 reports; can share data between reports to reduce the number of database accesses
Crystal Reports 2013 Scheduling Service	Crystal Reports Services	Adaptive Job Server	Runs scheduled legacy Crystal Reports jobs and publishes the results to an output location
Crystal Reports 2013 Viewing and Modification Service	Crystal Reports Services	Report Application Server (RAS)	Processes viewing and modification requests for Crystal Reports 2013 reports.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service	Service category	Server type	Service description
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	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 Analysis (formerly Voyager) crosstabs and charts
Native Connectivity Service	Connectivity Services	Connection Server	Provides Native Connectivity services for 64-bit architecture
Native Connectivity Service (32-bit)	Connectivity Services	Connection Server	Provides Native Connectivity services for 32-bit architecture
Output Filestore Service	Core Services	Output File Repository Server	Maintains a collection of completed documents
Platform Search Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled search to index all content in the Central Management Server (CMS) repository
Platform Search Service	Core Services	Adaptive Processing Server	Provides searching functionality for the BI platform
Probe Scheduling Service	Core Services	Adaptive Job Server	Provides scheduled Probe jobs and publishes the results to an output location
Program Scheduling Service	Core Services	Adaptive Job Server	Runs programs that have been scheduled to run at a given time
Publication Scheduling Service	Core Services	Adaptive Job Server	Runs scheduled publishing jobs and publishes the results to an output location
Publishing Post Processing Service	Core Services	Adaptive Processing Server	Performs actions on reports after they have completed, such as sending a report to an output location
Publishing Service	Core Services	Adaptive Processing Server	Coordinates with the Publishing Post Processing Service and Destination Job Service to publish reports to an output location, such as a file system, FTP server, email, or a user's inbox

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service	Service category	Server type	Service description
Rebean Service	Web Intelligence Services	Adaptive Processing Server	SDK used by Web Intelligence and Explorer
Replication Service	Core Services	Adaptive Job Server	Runs scheduled federation jobs to replicate content between federated sites
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
Security Token Service	Core Services	Adaptive Processing Server	SAP Single Sign-On support
Translation Service	Core Services	Adaptive Processing Server	Translates InfoObjects with input from the Translation Manager client
Users and Groups Import Scheduling Service	Core Services	Adaptive Job Server	Allows scheduling of principal file imports
Visual Difference Scheduling Service	Lifecycle Management Services	Adaptive Job Server	Runs scheduled Visual Difference (Lifecycle Management) jobs and publishes the results to an output location
Visual Difference Service	Lifecycle Management Services	Adaptive Processing Server	Determines whether documents are visually identical for doc promotion and Lifecycle Management
Visualization Service	Web Intelligence Services	Adaptive Processing Server	A common Visualization Object Model Service used by Web Intelligence
Web Intelligence Common Service	Web Intelligence Services	Web Intelligence Processing Server	Supports Web Intelligence documents processing
Web Intelligence Core Service	Web Intelligence Services	Web Intelligence Processing Server	Supports Web Intelligence documents processing
Web Intelligence Processing Service	Web Intelligence Services	Web Intelligence Processing Server	Accepts and processes Web Intelligence documents
Web Intelligence Scheduling Service	Web Intelligence Services	Adaptive Job Server	Enables support for scheduled Web Intelligence jobs
Web Services SDK and QaaWs	Core Services	Web Application Container Server	Web Services on WACS

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.2.3 Service categories

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

Table 5:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service category	Service	Server type
Core Services	Single Sign-on Service*	Central Management Server, Connection Server, Crystal Reports Processing Server, RAS, Dashboards Processing Server, and Web Intelligence Processing Server
Core Services	TraceLog Service*	Any server
Core Services	Translation Service	Adaptive Processing Server
Core Services	Users and Groups Import Scheduling Service*	Adaptive Job Server
Core Services	Web Application Container Service*	Web Application Container Server
Crystal Reports Services	Crystal Reports 2013 Processing Service	Crystal Reports Processing Server
Crystal Reports Services	Crystal Reports 2013 Scheduling Service	Adaptive Job Server
Crystal Reports Services	Crystal Reports 2013 Viewing and Modification Service	Report Application Server (RAS)
Crystal Reports Services	Crystal Reports Cache Service	Crystal Reports Cache Server
Crystal Reports Services	Crystal Reports Processing Service	Crystal Reports Processing Server
Crystal Reports Services	Crystal Reports Scheduling Service	Adaptive Job Server
Dashboards Services	Dashboards Cache Service	Dashboards Cache Server
Dashboards Services	Dashboards Processing Service	Dashboards Processing Server
Data Federation Services	Data Federation 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
Lifecycle Management Services	Visual Difference Scheduling Service	Adaptive Job Server
Lifecycle Management Services	Visual Difference Service	Adaptive Processing Server
Web Intelligence Services	Custom Data Access Service	Adaptive Processing Server
Web Intelligence Services	Document Recovery Service	Adaptive Processing Server
Web Intelligence Services	DSL Bridge Service	Adaptive Processing Server
Web Intelligence Services	Excel Data Access Service	Adaptive Processing Server
Web Intelligence Services	Information Engine Service	Web Intelligence Processing Server
Web Intelligence Services	Rebean Service	Adaptive Processing Server
Web Intelligence Services	Visualization Service	Adaptive Processing Server
Web Intelligence Services	Web Intelligence Common Service	Web Intelligence Processing Server
Web Intelligence Services	Web Intelligence Core Service	Web Intelligence Processing Server
Web Intelligence Services	Web Intelligence Monitoring Service*	Adaptive Processing Server

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service category	Service	Server type
Web Intelligence Services	Web Intelligence Processing Service	Web Intelligence Processing Server
Web Intelligence Services	Web Intelligence Scheduling Service	Adaptive Job Server

3.2.4 Server types

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

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

Table 6:

Server type	Service	Service category
Any server	TraceLog Service*	Core Services
Adaptive Job Server	Authentication Update Scheduling Service	Core Services
Adaptive Job Server	Crystal Reports 2013 Scheduling Service	Crystal Reports Services
Adaptive Job Server	Crystal Reports Scheduling Service	Crystal Reports Services
Adaptive Job Server	Destination Configuration Service*	Core Services
Adaptive Job Server	Destination Delivery Scheduling Service	Core Services
Adaptive Job Server	Lifecycle Management Scheduling Service	Lifecycle Management Services
Adaptive Job Server	Platform Search Scheduling Service	Core Services
Adaptive Job Server	Probe Scheduling Service	Core Services
Adaptive Job Server	Program Scheduling Service	Core Services
Adaptive Job Server	Publication Scheduling Service	Core Services
Adaptive Job Server	Replication Service	Core Services
Adaptive Job Server	Security Query Scheduling Service	Core Services
Adaptive Job Server	Users and Groups Import Scheduling Service*	Core Services
Adaptive Job Server	Visual Difference Scheduling Service	Lifecycle Management Services
Adaptive Job Server	Web Intelligence Scheduling Service	Web Intelligence Services
Adaptive Processing Server	Adaptive Connectivity Service	Connectivity Services
Adaptive Processing Server	BEx Web Application Service	Analysis Services
Adaptive Processing Server	Client Auditing Proxy Service	Core Services

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Server type	Service	Service category
Adaptive Processing Server	Custom Data Access Service	Web Intelligence Services
Adaptive Processing Server	Data Federation Service	Data Federation Services
Adaptive Processing Server	Document Recovery Service	Web Intelligence Services
Adaptive Processing Server	DSL Bridge Service	Web Intelligence Services
Adaptive Processing Server	Excel Data Access Service	Web Intelligence Services
Adaptive Processing Server	Insight to Action Service	Core Services
Adaptive Processing Server	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	Analysis Services
Adaptive Processing Server	Platform Search Service	Core Services
Adaptive Processing Server	Publishing Post Processing Service	Core Services
Adaptive Processing Server	Publishing Service	Core Services
Adaptive Processing Server	Rebean Service	Web Intelligence Services
Adaptive Processing Server	Security Token Service	Core Services
Adaptive Processing Server	Translation Service	Core Services
Adaptive Processing Server	Visual Difference Service	Lifecycle Management Services
Adaptive Processing Server	Visualization Service	Web Intelligence Services
Adaptive Processing Server	Web Intelligence Monitoring Service*	Web Intelligence Services
Central Management Server	Central Management Service	Core Services
Central Management Server	Single Sign-on Service*	Core Services
Connection Server	Native Connectivity Service	Connectivity Services
Connection Server	Native Connectivity Service (32-bit)	Connectivity Services
Connection Server	Single Sign-on Service*	Core Services
Crystal Reports Cache Server	Crystal Reports Cache Service	Crystal Reports Services
Crystal Reports Processing Server	Crystal Reports 2013 Processing Service	Crystal Reports Services
Crystal Reports Processing Server	Crystal Reports Processing Service	Crystal Reports Services
Crystal Reports Processing Server	Single Sign-on Service*	Core Services
Dashboards Cache Server	Dashboards Cache Service	Dashboards Services
Dashboards Processing Server	Dashboards Processing Service	Dashboards Services
Dashboards Processing Server	Single Sign-on Service*	Core Services
Dashboard Server	Dashboard Service	Core Services
Event Server	Event Service	Core Services
Input File Repository Server	Input Filestore Service	Core Services

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Server type	Service	Service category
Output File Repository Server	Output Filestore Service	Core Services
Report Application Server (RAS)	Crystal Reports 2013 Viewing and Modification Service	Crystal Reports Services
RAS	Single Sign-on Service*	Core Services
Web Application Container Server	RESTful Web Service	Core Services
Web Application Container Server	Web Application Container Service*	Core Services
Web Intelligence Processing Server	Information Engine Service	Web Intelligence Services
Web Intelligence Processing Server	Single Sign-on Service*	Core Services
Web Intelligence Processing Server	Web Intelligence Common Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Core Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Processing Service	Web Intelligence Services

Table 7:

Server type	Service	Service category
Adaptive Job Server	Authentication Update Scheduling Service	Core Services
Adaptive Job Server	Crystal Reports 2013 Scheduling Service	Crystal Reports Services
Adaptive Job Server	Crystal Reports Scheduling Service	Crystal Reports Services
Adaptive Job Server	Destination Delivery Scheduling Service	Core Services
Adaptive Job Server	Lifecycle Management Scheduling Service	Lifecycle Management Services
Adaptive Job Server	Platform Search Scheduling Service	Core Services
Adaptive Job Server	Probe Scheduling Service	Core Services
Adaptive Job Server	Program Scheduling Service	Core Services
Adaptive Job Server	Publication Scheduling Service	Core Services
Adaptive Job Server	Replication Service	Core Services
Adaptive Job Server	Security Query Scheduling Service	Core Services
Adaptive Job Server	Visual Difference Scheduling Service	Lifecycle Management Services
Adaptive Job Server	Web Intelligence Scheduling Service	Web Intelligence Services
Adaptive Processing Server	Adaptive Connectivity Service	Connectivity Services
Adaptive Processing Server	BEx Web Application Service	Analysis Services
Adaptive Processing Server	Client Auditing Proxy Service	Core Services
Adaptive Processing Server	Custom Data Access Service	Web Intelligence Services
Adaptive Processing Server	Data Federation Service	Data Federation Services
Adaptive Processing Server	Document Recovery Service	Web Intelligence Services
Adaptive Processing Server	DSL Bridge Service	Web Intelligence Services

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Server type	Service	Service category
Adaptive Processing Server	Excel Data Access Service	Web Intelligence Services
Adaptive Processing Server	Insight to Action Service	Core Services
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	Analysis Services
Adaptive Processing Server	Platform Search Service	Core Services
Adaptive Processing Server	Publishing Post Processing Service	Core Services
Adaptive Processing Server	Publishing Service	Core Services
Adaptive Processing Server	Rebean Service	Web Intelligence Services
Adaptive Processing Server	Security Token Service	Core Services
Adaptive Processing Server	Translation Service	Core Services
Adaptive Processing Server	Visual Difference Service	Lifecycle Management Services
Adaptive Processing Server	Visualization Service	Web Intelligence Services
Central Management Server	Central Management Service	Core Services
Connection Server	Native Connectivity Service	Connectivity Services
Connection Server	Native Connectivity Service (32-bit)	Connectivity Services
Crystal Reports Cache Server	Crystal Reports Cache Service	Crystal Reports Services
Crystal Reports Processing Server	Crystal Reports 2013 Processing Service	Crystal Reports Services
Crystal Reports Processing Server	Crystal Reports Processing Service	Crystal Reports Services
Dashboards Cache Server	Dashboards Cache Service	Dashboards Services
Dashboards Processing Server	Dashboards Processing Service	Dashboards Services
Dashboard Server	Dashboard Service	Core Services
Event Server	Event Service	Core Services
Input File Repository Server	Input Filestore Service	Core Services
Output File Repository Server	Output Filestore Service	Core Services
Report Application Server (RAS)	Crystal Reports 2013 Viewing and Modification Service	Crystal Reports Services
Web Application Container Server	RESTful Web Service	Core Services
Web Intelligence Processing Server	Information Engine Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Common Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Core Service	Web Intelligence Services
Web Intelligence Processing Server	Web Intelligence Processing Service	Web Intelligence Services

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.2.5 Servers

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

Server	Description
Adaptive Job Server	A generic server that processes scheduled jobs. When you add a Job server to the BI platform system, you can configure the Job server to process reports, documents, programs, or publications and send the results to different destinations.
Adaptive Processing Server	A generic server that hosts services responsible for processing requests from a variety of sources. The installation program installs one Adaptive Processing Server (APS) per host system. Depending on the features that you've installed, this APS may host a large number of services, such as the Monitoring Service, Lifecycle Management Service, Multi-Dimensional Analysis Service (MDAS), Publishing Service, and others. For production or test systems, the best practice is to create additional APSs, and configure the APSs to meet your business requirements. For more information, see Introduction to the System Configuration Wizard [page 78] and Configuring Adaptive Processing Servers for production systems [page 351].
Central Management Server (CMS)	Maintains a database of information about your BI platform system (in the CMS system database) and audited user actions (in the Auditing Data Store). All platform services are managed by the CMS. The CMS also controls access to the system files where documents are stored, and information on users, user groups, security levels (including authentication and authorization), and content.
Connection Server	Provides database access to source data. It supports relational databases, as well as OLAP and other formats. The Connection Server is responsible for handling connection and interaction with the various data sources and providing a common feature set to clients.
Crystal Reports Cache Server	Intercepts report requests sent from clients to the page server. If the cache server cannot fulfill the request with a cached report page, it passes the request on to the Crystal Reports Processing server, which runs the report and returns the results. The cache server then caches the report page for potential future use.
Crystal Reports Processing Server	Responds to page requests by processing reports and generating encapsulated page format (EPF) pages. The key benefit of EPF is that it supports page-on-demand access, so only the requested page is returned, not the entire report. This improves system performance and reduces unnecessary network traffic for large reports.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

3.3 Client applications

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Examples of this type of application include: Crystal Reports and Live Office.

> **Note**
>
> Although Live Office is a rich functionality application, it interfaces with BI platform web services over HTTP.

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

3.3.1 Installed with SAP BusinessObjects Business Intelligence platform Client Tools

3.3.1.1 Web Intelligence Rich Client

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

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

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

3.3.1.2 Business View Manager

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.3.1.3 Report Conversion Tool

The Report Conversion Tool converts reports to Web Intelligence format and publishes them to a Central Management Server (CMS).

Reports can be retrieved from the CMS folders `Public`, `Favorites`, or `Inbox`. Once converted, reports publish to the same folder as the original Web Intelligence report, or to a different folder. The tool does not convert all Web Intelligence features and reports. The level of conversion depends on the features in the original report. Some features prevent the report from being converted. Other features are modified, reimplemented, or removed by the tool during conversion.

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

3.3.1.4 Universe design tool

Universe design tool (formerly Universe Designer) allows data designers to combine data from multiple sources in a semantic layer that hides database complexity from end users. It abstracts the complexity of data by using business rather than technical language to access, manipulate, and organize data.

Universe design tool provides a graphical interface to select and view tables in a database. The database tables are represented as table symbols in a schema diagram. Designers can use this interface to manipulate tables, create joins between tables, create alias tables, create contexts, and solve loops in a schema.

You can also create universes from metadata sources. Universe design tool is used for the universe generation at the end of the creation process.

3.3.1.5 Query as a Web Service

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

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

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

- Server component
  The server component (included in the BI platform) stores the Query as a Web Service catalog and hosts the published web services.
- Client tool
  This is how business users create and publish their queries as a web service on the server. You can install the client tool on several machines that can access and share the same catalog stored on the server. The client tool communicates with the server components via web services.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Microsoft Office, Excel, and InfoPath
- SAP NetWeaver Technology Platform
- OpenOffice
- Business rules and process management applications
- Enterprise Service Bus platforms

3.3.1.6 Information design tool

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

3.3.1.7 Translation Management Tool

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

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

Translation Management Tool:

- Translates universe or documents for a multilingual audience.
- Defines the metadata language parts of a document, and the appropriate translation. It generates external XLIFF format and imports XLIFF files to get translated information.
- Lists the universe or document structure to be translated.
- Lets you translate the metadata through the user interface, or through an external translation tool by importing and exporting XLIFF files.
- Creates multilingual documents.

3.3.1.8 Data Federation Administration Tool

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

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

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

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

- Test SQL queries.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

3.3.1.9 Widgets for the BI Platform

Widgets are mini-applications that allow easy and fast access to frequently used functions and provide visual information from your desktop. Widgets for the BI platform (formerly BI Widgets) allow your organization to provide access to existing Business Intelligence (BI) content on the BI platform, or you can add Web Dynpro applications that are registered as XBCML (Extensible Business Client Markup Language) widgets on the SAP NetWeaver Application Server components as desktop widgets.

To render XBCML widgets on the user's desktop, SAP Web Dynpro Flex Client is used. The SAP Web Dynpro Flex Client is a rendering engine based on Adobe Flex which is used for rendering widgets. For details about how to configure Web Dynpro applications, see the *To enable widgets on the SAP NetWeaver Application Server components* topic in the *Widgets for SAP BusinessObjects User Guide.*

> **Note**
>
> The SAP Web Dynpro Flex Client support for XBCML Widgets begins in release 7.0 EhP2 SP3. Flex Client queue support is confined only to Flex Client issues found in XBCML widgets in these specified releases.

With widgets, you search or browse for existing content, such as Web Intelligence documents, Dashboards models, and Web Dynpro applications, then paste the information onto your desktop so it is available when needed.

As a widget, the content gains the following features from the widget framework:

- User-controlled size and positioning
- Automatic refresh
- Optional setting as the top application window
- Full BI platform security (Web Intelligence report parts and Dashboards models only)
- Saved display
- Saved data context state (Web Intelligence report parts only)
- Web Intelligence OpenDocument links to detailed reports (Web Intelligence documents only)
- Tabbed views (Dashboards models only)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.3.2 Installed with SAP BusinessObjects Business Intelligence platform

3.3.2.1 Central Configuration Manager (CCM)

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

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

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

3.3.2.2 Upgrade management tool

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

For information on upgrading from a previous version of the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Upgrade Guide*.

3.3.2.3 Repository Diagnostic Tool

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.3.3 Available separately

3.3.3.1 SAP BusinessObjects Analysis, edition for Microsoft Office

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

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

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

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

3.3.3.2 SAP Crystal Reports

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

3.3.3.3 SAP BusinessObjects Dashboards

SAP BusinessObjects Dashboards (formerly Xcelsius) is a tool for data visualization and the creation of dynamic, interactive dashboards. Data and formulae are imported or directly entered into an embedded Excel spreadsheet. A Flash interface provides a canvas that can display a variety of analytics and dashboards.

Data can be updated dynamically from the BI platform, and exported to a variety of different formats that can be viewed by data consumers in standard formats, such as PowerPoint, PDF, or Flash.

3.3.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer is a data discovery application that uses a powerful search capability to retrieve answers to business questions from corporate data quickly and directly.

When you install SAP BusinessObjects Explorer, the following servers are added to the BI platform Central Configuration Manager (CCM) and Central Management Console (CMC):

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Explorer Master Server: manages all of the Explorer servers.
- Explorer Indexing Server: provides and manages the indexing of information space data and metadata.
- Explorer Search Server: processes search queries and returns the results.
- Explorer Exploration Server: provides and manages the information space exploration and analysis capabilities including search on data, filtering and aggregation.

3.3.3.5 SAP Lumira

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

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

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

3.3.4 Web application clients

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

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

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

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

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

3.3.4.1 Central Management Console (CMC)

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

3.3.4.2 BI launch pad

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

BI launch pad allows users to manage:

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

3.3.4.3 BI workspaces

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

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

> **Note**
>
> BI workspaces is an integral part of the BI launch pad application. Therefore, to use the BI workspaces features, you must purchase an SAP BusinessObjects Business Intelligence platform license that includes BI launch pad as part of the agreement.

3.3.4.4 Report viewers

Each report viewer supports a different platform and a different browser. Preferences can be set in BI launch pad and the Central Management Console (CMC). There are two categories of viewers:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Zero-client report viewers (DHTML viewer)
  Zero-client report viewers reside on the web application server. When a user requests a report, the web application server retrieves the report pages from the BI platform and creates DHTML pages that display in the web browser. To choose the zero-client report (DHTML) viewer, select *Preferences* > *Crystal Reports* > *Web (no downloading required)*
- Client-side report viewers (Active X viewer, Java viewer)
  Client-side report viewers are downloaded and installed in the user's browser. When a user requests a report, the application server processes the request, and retrieves the report pages from the BI platform. The web application server then passes the report pages to the client-side viewer, which processes the report pages and displays them in the web browser. To choose a client-side report viewer, select *Preferences* > *Crystal Reports* > *Web ActiveX (ActiveX required)* or *Web Java (Java required)*.

All report viewers process report requests and present report pages that appear in the web browser.

> **Note**
>
> For online access of Crystal reports through the Central Management Console, it is recommended to use the default DHTML web viewer. Avoid using the legacy Java viewer, which does not provide the same functionality as the DHTML viewer.

For more information on the functionality or platform support provided by each report viewer, see the *BI Launch Pad User Guide*, the *Report Application Server .NET SDK Developer Guide*, or the *Viewers Java SDK Developer Guide*.

3.3.4.5 SAP BusinessObjects Web Intelligence

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

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

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

3.3.4.6 SAP BusinessObjects Analysis, edition for OLAP

SAP BusinessObjects Analysis, edition for OLAP (formerly Voyager) is an online analytical processing (OLAP) tool in the BI launch pad portal for working with multi-dimensional data. It can also combine information from different OLAP data sources within a single workspace. Supported OLAP providers include SAP BW and Microsoft Analysis Services.

The Analysis OLAP feature set combines elements of SAP Crystal Reports (direct data access to OLAP cubes for production reporting) and SAP BusinessObjects Web Intelligence (ad-hoc analytic reporting with universes from OLAP data sources). It offers a range of business and time calculations, and includes features such as time sliders to make the analysis of OLAP data as simple as possible.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The Analysis, edition for OLAP web application is available only as a Java web application. There is no corresponding application for .NET.

3.3.4.7 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile allows your users to remotely access the same business intelligence (BI) reports, metrics, and real-time data available on desktop clients from a wireless device. Content is optimized for mobile devices so your users can easily access, navigate, and analyze familiar reports without additional training.

With SAP BusinessObjects Mobile, management and information workers can stay up-to-date and make decisions using the latest information. Sales and field service staff can provide the right customer, product, and work order information where and when it's needed.

SAP BusinessObjects Mobile supports a broad set of mobile devices including BlackBerry, Windows Mobile, and Symbian.

For information on mobile installation, configuration, and deployment, see the *SAP BusinessObjects Mobile Installation and Deployment Guide*. For information on using SAP BusinessObjects Mobile, see the *Using SAP BusinessObjects Mobile Guide*.

3.4 Process Workflows

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

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

3.4.1 Startup and authentication

3.4.1.1 Logging on to the BI platform

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

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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

3.4.1.2 SIA start-up

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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.4.1.3 SIA shutdown

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

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

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.

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

3.4.2 Program objects

3.4.2.1 Setting a schedule for a program object

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

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

3.4.2.2 A scheduled program object runs

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

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

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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. The Program Scheduling Service communicates with the Input File Repository Server (FRS) to obtain the program object.

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

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

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

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

3.4.3 Crystal Reports

3.4.3.1 Viewing a cached SAP Crystal report page

This workflow describes the process of a user requesting a page in an SAP Crystal report (for example from the report viewer in BI launch pad), when the report page already exists on a cache server. This workflow applies to both SAP Crystal Reports 2013 and SAP Crystal Reports for Enterprise.

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.4.3.2 Viewing a non-cached SAP Crystal Reports 2013 page

This workflow describes the process of a user requesting a page in an SAP Crystal Reports 2013 report (for example from the report viewer in BI launch pad), when the page does not already exist on a cache server.

> **Note**
>
> This workflow requires the CMS, Crystal Reports Cache Server, Crystal Reports 2013 Processing Server, and Output File Repository Server to be running.

1. The user sends the view request through the web server to the web application server.
2. The web application server interprets the request, determines that it is a request to view a selected report page, and sends a request to the Central Management Server (CMS) to ensure that the user has sufficient rights to view the report.
3. The CMS checks the CMS system database to verify the user has sufficient rights to view the report.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the report.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the page of the report (`.epf` file).
6. The Crystal Reports Cache Server determines if the requested file exists in the cache directory.
   In this example, the requested `.epf` file is not found in the cache directory.
7. The Crystal Reports Cache Server sends the request to the Crystal Reports 2013 Processing Server.
8. The Crystal Reports 2013 Processing Server queries the Output File Repository Server (FRS) for the requested report instance, and the Output FRS sends the requested report instance to the Crystal Reports 2013 Processing Server.

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

9. The Crystal Reports 2013 Processing Server opens the report instance and checks the report to determine if it has data.

   The Crystal Reports 2013 Processing Server determines that the report contains data, and creates the `.epf` file for the requested report page without having to connect to the production database.
10. The Crystal Reports 2013 Processing Server sends the `.epf` file to the Crystal Reports Cache Server.
11. The Crystal Reports Cache Server writes the `.epf` file to the cache directory.
12. The Crystal Reports Cache Server sends the requested page to the web application server.
13. The web application server sends the page to the web client via the web server, where the page is rendered and displayed.

3.4.3.3 Viewing an SAP Crystal Reports 2013 report on demand

This workflow describes the process of a user requesting an SAP Crystal Reports 2013 report page on demand to see the latest data; for example, from the report viewer in BI launch pad.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> This workflow requires the CMS, Crystal Reports Cache Server, Crystal Reports 2013 Processing Server, and Input File Repository Server to be running.

1. The user sends the view request through the web server to the web application server.
2. The web application server interprets the request and determines that it is a request to view a selected report page. The web application server sends a request to the Central Management Server (CMS) to ensure that the user has sufficient rights to view the report.
3. The CMS checks the CMS system database to verify the user has sufficient rights to view the report.
4. The CMS sends a response to the web application server to confirm the user has sufficient rights to view the report.
5. The web application server sends a request to the Crystal Reports Cache Server requesting the page of the report (`.epf` file).
6. The Crystal Reports Cache Server checks to see if the page already exists. Unless the report meets the requirements for on demand report sharing (within a set time of another on demand request, database login, parameters), the Crystal Reports Cache Server sends a request for the Crystal Reports 2013 Processing Server to generate the page.
7. The Crystal Reports 2013 Processing Server requests the report object from the Input File Repository Server (FRS). The Input FRS streams a copy of the object to the Crystal Reports 2013 Processing Server.

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

8. The Crystal Reports 2013 Processing Server opens the report in its memory and checks to see if the report contains data. In this example, there is no data in the report object, so the Crystal Reports 2013 Processing Server connects to the data source to retrieve data and generate the report.
9. The Crystal Reports 2013 Processing Server sends the page (`.epf` file) to the Crystal Reports Cache Server. The Crystal Reports Cache Server stores a copy of the `.epf` file in its cache directory in anticipation of new viewing requests.
10. The Crystal Reports Cache Server sends the page to the web application server.
11. The web application server sends the page to the web client via the web server, where the page is rendered and displayed.

3.4.3.4 Setting a schedule for an SAP Crystal report

This workflow describes the process of a user scheduling an SAP Crystal report to be run at a future time from a web application such as the Central Management Console (CMC) or BI launch pad. This workflow applies to both SAP Crystal Reports 2013 and SAP Crystal Reports for Enterprise.

1. The web client submits a schedule request in a URL via the web server to the web application server.
2. The web application server interprets the URL request and determines that the request is a schedule request. The web application server sends the schedule time, database login values, parameter values, destination, and format to the specified Central Management Server (CMS).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. The CMS ensures that the user has rights to schedule the object. If the user has sufficient rights, the CMS adds a new record to the CMS system database. The CMS also adds the instance to its list of pending schedules.
4. The CMS sends a response to the web application server to let it know that the schedule operation was successful.
5. The web application server generates the next HTML page and sends it via the web server to the web client.

3.4.3.5 A scheduled SAP Crystal Reports 2013 report runs

This workflow describes the process of a scheduled SAP Crystal Reports 2013 report 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 Crystal Reports 2013 Scheduling Service running on an Adaptive Job Server (based on the *Maximum Jobs Allowed* value configured on each Adaptive Job Server). The CMS sends the job information (report ID, format, destination, logon information, parameters, and selection formulas) to the Crystal Reports 2013 Scheduling Service.
3. The Crystal Reports 2013 Scheduling Service communicates with the Input File Repository Server (FRS) to obtain a report template as per the requested report ID.

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

4. The Crystal Reports 2013 Scheduling Service starts the JobChildserver process.
5. The child process (JobChildserver) starts `ProcReport.dll` when it receives the template from the Input File Repository Server. `ProcReport.dll` contains all of the parameters that were passed from the CMS to the Crystal Reports 2013 Scheduling Service.
6. `ProcReport.dll` starts `crpe32.dll`, which processes the report according to the parameters passed.
7. While `crpe32.dll` is still processing the report, records are retrieved from the data source as defined in the report.
8. The Crystal Reports 2013 Scheduling Service updates the CMS periodically with the job status. The current status is Processing.
9. Once the report is compiled into the memory of the Crystal Reports 2013 Scheduling Service, it may be exported to a different format, such as Portable Document Format (PDF). When exporting to PDF, `crxfpdf.dll` is used.
10. The report with saved data is submitted to the scheduled location (such as email), and then it is sent to the Output FRS.

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

11. The Crystal Reports 2013 Scheduling Service updates the CMS with the job status. The current status is Success.
12. The CMS updates the job status in its memory and then writes the instance information to the CMS system database.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3.4.4 Web Intelligence

3.4.4.1 Viewing an SAP BusinessObjects Web Intelligence document on demand

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

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

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

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

3.4.4.2 Setting a schedule for an SAP BusinessObjects Web Intelligence document

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

3.4.4.3 A scheduled SAP BusinessObjects Web Intelligence document runs

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

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

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

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

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

7. The Web Intelligence Processing Server notifies the Web Intelligence Scheduling Service (on the Adaptive Job Server) that document creation is completed. If the document is scheduled to go to a destination (file system,

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

FTP, SMTP, or Inbox), the Adaptive Job Server retrieves the processed document from the Output FRS and delivers it to the specified destination(s). Assume that this is not the case in this example.

8. The Web Intelligence Scheduling Service updates the CMS with the job status.
9. The CMS updates the job status in its memory, and then writes the instance information to the CMS system database.

3.4.5 Analysis

3.4.5.1 Viewing an SAP BusinessObjects Analysis, edition for OLAP workspace

This workflow describes the process of a user requesting to view an SAP BusinessObjects Analysis, edition for OLAP workspace from BI launch pad.

> **Note**
>
> This workflow requires the CMS, Adaptive Processing Server (containing the Multi-Dimensional Analysis Service (MDAS)), and Input File Repository Server to be running.

1. The web client sends a request via the web server to the web application server to view a new workspace. The web client communicates with the web application server using DHTML AJAX technology (Asynchronous JavaScript and XML). The AJAX technology allows for partial page updates, so a new page does not have to be rendered for each new request.
2. The web application server translates the request and sends it to the Central Management Server (CMS) to determine whether a user is entitled to view or create a new workspace.
3. The CMS retrieves the user's credentials from the CMS system database.
4. If the user is allowed to view or create a workspace, the CMS confirms this to the web application server. At the same time, it also sends a list of one or more available Multi-Dimensional Analysis Services (MDAS).
5. The web application server picks an MDAS from the list of available choices and sends a CORBA request to the service to find the appropriate OLAP server(s) to create a new, or refresh an existing, workspace.
6. The MDAS needs to communicate with the Input File Repository Server (FRS) to retrieve the appropriate workspace document that has information about the underlying OLAP database and an initial OLAP query saved with it. The Input FRS retrieves the appropriate Analysis workspace from the underlying directory and streams that workspace back to the MDAS.
7. The MDAS opens the workspace, formulates a query, and sends it to the OLAP database server. The MDAS has to have an appropriate OLAP database client configured for the OLAP data source. The translation of the web client query into the appropriate OLAP query needs to occur. The OLAP database server sends the query result back to the MDAS.
8. The MDAS, based on the request to either create, view, print, or export, pre-renders the result to enable the Java WAS to finish the rendering more quickly. The MDAS sends XML packages of the rendered result back to the web application server.
9. The web application server renders the workspace and sends the formatted page or portion of the page to the web client via the web server. The web client displays the updated or newly requested page. This is a zero-client solution that does not need to download any Java or ActiveX components.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4 System Configuration Wizard

4.1 Introduction to the System Configuration Wizard

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

Important benefits of using the wizard:

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

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

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

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

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

4.2 Specifying the products you use

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

The wizard configures product servers as follows:

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

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

4.3 Choosing a deployment template

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

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

Choosing an appropriate deployment template is important for several reasons:

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

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

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

> **Note**
>
> RAM Required is the minimum amount of RAM required for BI platform servers. For example, on a machine with 16 GB of RAM, where the operating system uses 1 GB of RAM, the database server uses another 1 GB, and BI platform servers use 10 GB, RAM Required equals 10 GB, not 12 GB or 16 GB. The RAM Required number

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

represents only a typical value; your system could need more RAM under heavy load. For optimal system performance, you should always perform system sizing.

> **Note**
>
> Whenever you open the *Capacity* page, the deployment template shown on the page represents the current system state, if the current system state matches one of the predefined deployment templates. For example, if you have manually created an extra Adaptive Processing Server using the CMC, the current state of your system doesn't match any of the deployment templates, so the *Capacity* page displays the *Keep existing configuration* check box to indicate that the system was configured outside of the wizard. In a multi-node deployment, the *Keep existing configuration* check box is also displayed if any node has a number of APSs not matching a deployment template, or if the number of APSs on different nodes is different. You can clear the check box if you want to use the wizard to change your configuration.

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

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

The DeploymentTemplates.pdf file

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4.4 Specifying data folder locations

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

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

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

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

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

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

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

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

Example scenarios:

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

4.5 Reviewing your changes

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

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

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

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

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

Related Information

Log files and response files [page 83]

4.6 Log files and response files

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

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

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

The log file contains the following content:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

Related Information

Using a response file [page 84]

4.6.1 Using a response file

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

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

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

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

Running the script

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

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

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

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

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

- `-help`: Display the command-line help.
- `-r`: Specify the path and name of the response file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

Examples

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

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

Sample response file

```
# ******************************************
# ***************** Products *****************
# ******************************************

# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the “Products.”
settings below.

Products.KeepExistingConfiguration = true

# The “Products.” settings below will be ignored if
Products.KeepExistingConfiguration = true.

# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI
platform.
# "false": the product's servers are not auto-started with BI platform.

# Crystal Reports
Products.crystalreports = true

# Analysis edition for OLAP
Products.olap = true

# Web Intelligence
Products.webintelligence = false

# Dashboards (Xcelsius)
Products.dashboards = false

# Data Federator
Products.datafederator = true

# Lifecycle Manager
Products.LCM = true
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
# ******************************************************
# ***************** Deployment Template *****************
# ******************************************************

# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and the
Capacity.DeploymentTemplate setting below will be ignored.
# "false": the deployment template configuration will be modified according to the
Capacity.DeploymentTemplate setting below.

Capacity.KeepExistingConfiguration = true

# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.

Capacity.DeploymentTemplate = xs


# ****************************************
# ***************** Folders *****************
# ****************************************

# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders."
settings below.

Folders.KeepExistingConfiguration = true

# The “Folders.” settings below will be ignored if
Folders.KeepExistingConfiguration = true.

# ------ All nodes use the same folders ------
# Use this section when you have one node, or when all nodes have the same folder
locations. Otherwise, comment it out.

Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>

# ------ Nodes use different folders ------
# Use this section when nodes have different folder locations. Otherwise, comment
it out.

# ------ NodeOne ------
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>

# ------ NodeTwo ------
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5 Managing Licenses

5.1 Managing license keys

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

Related Information

To view license information [page 88]
To add a license key [page 88]
To view current account activity [page 89]

5.1.1 To view license information

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

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

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

Related Information

To add a license key [page 88]
To view current account activity [page 89]

5.1.2 To add a license key

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

The key is added to the list.

Related Information

To view license information [page 88]
To view current account activity [page 89]

5.1.3 To view current account activity

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

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

Related Information

To add a license key [page 88]
To view license information [page 88]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6 Managing Users and Groups

6.1 Account management overview

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

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

6.1.1 User management

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

Table 8: Default user accounts

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

Note

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

6.1.2 Group management

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 9: Default group accounts

Account name	Description
Administrators	Members of this group can perform all tasks in all of the BI platform applications (CMC, CCM, Publishing Wizard, and BI launch pad). By default, the *Administrators* group contains only the Administrator user.
Everyone	Each user is a member of the *Everyone* group.
QaaWS Group Designer	Members of this group have access to Query as a Web Service.
Report Conversion Tool Users	Members of this group have access to the Report Conversion Tool application.
Translators	Members of this group have access to the Translation Manager application.
Universe Designer Users	Users who belong to this group are granted access to the *Universe Designer* folder and the *Connections* folder. They can control who has access rights to the Designer application. You must add users to this group as needed. By default, no user belongs to this group.

Related Information

How rights work in BI platform [page 112]
Granting access to users and groups [page 101]

6.1.3 Available authentication types

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 10: Authentication types

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2 Managing Enterprise and general accounts

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

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

6.2.1 To create a user account

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

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

How rights work in BI platform [page 112]

6.2.2 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 Information

To create a new alias for an existing user [page 109]

6.2.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

   The delete confirmation dialog box appears.
4. Click *OK*.
   The user account is deleted.

Related Information

To modify a user account [page 94]
To disable an alias [page 111]

6.2.4 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 BI platform content.

6.2.5 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Modify the properties for the group.

   Click the links from the navigation list to access different dialog boxes and modify different properties.

   - If you want to change the title or description for the group, click *Properties*.
   - If you want to modify the rights that principals have to the group, click *User Security*.
   - If you want to modify profile values for group members, click *Profile Values*.
   - If you want to add the group as a subgroup to another group, click *Member Of*.
4. Click *Save*.

6.2.6 To view group members

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.

6.2.7 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 Information

To specify group membership [page 97]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2.8 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.

6.2.9 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.

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2.10 To add users or user groups in bulk

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

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

The following conditions apply to the bulk addition process:

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

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

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

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

The users or user groups are imported to the CMC.

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

6.2.11 To enable the Guest account

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2.12 Adding users to groups

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

You can add users to groups in the following ways:

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

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

Related Information

To specify group membership [page 97]

6.2.12.1 Adding a user to one or more user groups

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

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

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

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

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

4. Click *OK*.

6.2.12.2 Adding one or more users to a user group

You can add multiple users to a user group.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

5. Click *OK*.

6.2.13 Changing password settings

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

6.2.13.1 To change user password settings

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*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2.13.2 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 11: Password settings

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

4. Click *Update*.

Inactive user accounts will not be automatically de-activated.

6.2.14 Granting access to users and groups

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

Related Information

To assign principals to an access control list for an object [page 121]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2.15 Controlling access to user inboxes

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

Related Information

Setting a schedule for a program object [page 70]
Managing security settings for objects in the CMC [page 120]
Type-specific rights [page 118]

6.2.16 Configuring BI launch pad options

In the CMC, administrators can configure BI launch pad preferences for user groups. By configuring properties in the `BOE.war` file, you can specify which information appears on a user's BI launch pad logon screen.

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

6.2.16.1 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 the users 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.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

```
authentication.visible=true
```

5. To change the default authentication, add the following line:

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

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

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

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

```
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 *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

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

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.2.16.2.1 Setting BI launch pad preferences for a user group

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

6.2.17 Managing attributes for system users

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

- Enterprise
- SAP
- LDAP
- Windows AD

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

- Full Name
- Email address

Attribute names

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

- *Name*
- *Internal name*

The “Name” property is the friendly identifier for the attribute and it is used to query filters when working with the Universe semantic layer. For more information, see the Universe Design tool documentation. The “Internal Name” is used by developers working with the BI platform SDK. This property is an automatically generated name.

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Prerequisites for expanding mapped user attributes

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

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

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

6.2.18 Prioritizing user attributes across multiple authentication options

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

Related Information

To configure the LDAP host [page 219]
To import SAP roles [page 279]
To map Windows AD users and groups [page 240]

6.2.19 To add a new user attribute

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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

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

   The BI platform does not provide a mechanism to automatically verify that the attribute name provided exists in the external directory. Ensure that the name provided is correct and valid.
7. Repeat steps 5-6 if additional sources are required for the new attribute.
8. Click *OK* to save and submit the new attribute to the BI platform.
   The new attribute Name, Internal Name, Source, and Attribute Source Name appear in the *User Attribute Management* management area of the CMC.

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

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

6.2.20 To edit customised user attributes

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

- The name of the attribute in the BI platform

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

- The attribute source name
- Additional sources for the attribute

1. Go to the *User Attribute Management* management area of the CMC.
2. Select the attribute you want to edit.
3. Click the *Edit selected attribute* icon.
   The *Edit* dialog box appears.
4. Modify the attribute Name or source information.
5. Click *OK* to save and submit the modifications to the BI platform.
   The modified values appear in the *User Attribute Management* management area of the CMC.

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

6.3 Managing aliases

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

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

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

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

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

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

1. Go to the *Users and Groups* management area of the CMC.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Click *Manage* > *New* > *New User*.
   The *New User* dialog box appears.
3. Select the authentication type for the user, for example, Windows AD.
4. Type in the third-party account name for the user, for example, **`bsmith`**.
5. Select the connection type for the user.
6. Click *Create & Close*.

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

6.3.2 To create a new alias for an existing user

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

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

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

   An alias is created for the user. When you view the user in the CMC, at least two aliases are shown, the one that was already assigned to the user and the one you just created.
8. Click *Save & Close* to exit the *Properties* dialog box.

6.3.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **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*.

6.3.4 To delete an alias

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6.3.5 To disable an alias

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

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

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

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

Related Information

To delete an alias [page 110]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

7 Setting Rights

7.1 How rights work in BI platform

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

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

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

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

Related Information

Rights override [page 116]

7.1.1 Access levels

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

Related Information

Working with access levels [page 125]

7.1.2 Advanced rights settings

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

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

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

Table 12: Rights options

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

Related Information

Type-specific rights [page 118]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

7.1.3 Inheritance

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

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

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

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

7.1.3.1 Group inheritance

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

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

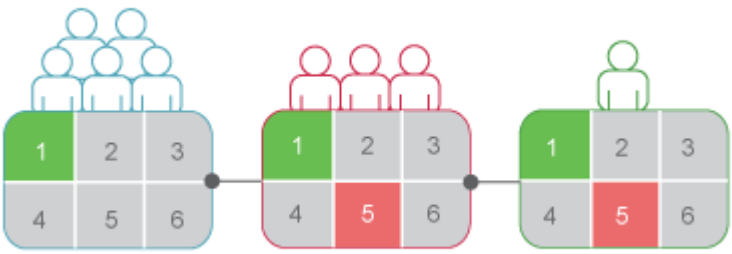


Figure 1: Group inheritance example 1

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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

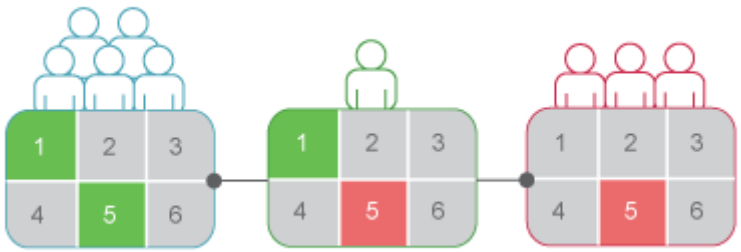


Figure 2: Group inheritance example 2

Related Information

Rights override [page 116]

7.1.3.2 Folder inheritance

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

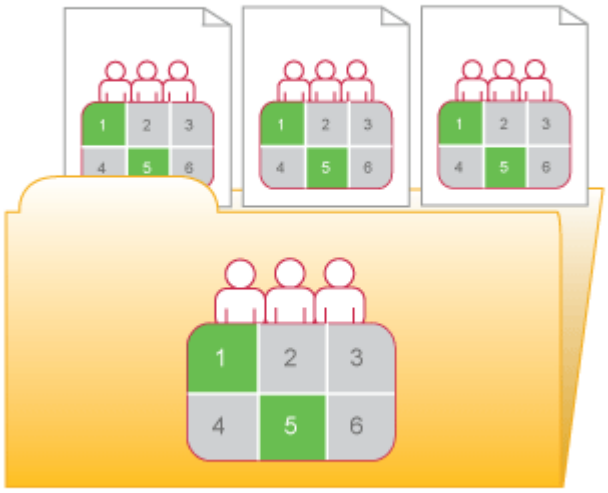


Figure 3: Folder inheritance example

Related Information

Rights override [page 116]

7.1.3.3 Rights override

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

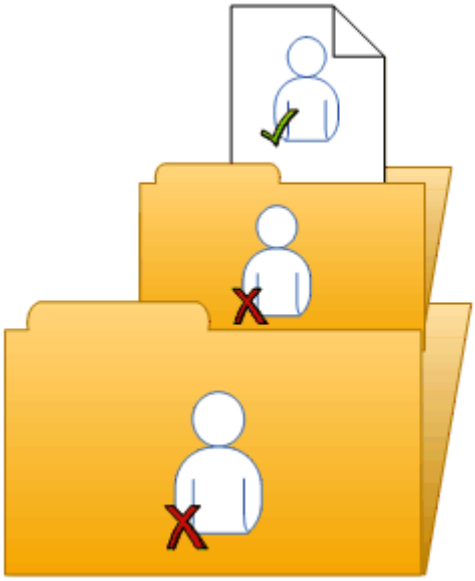


Figure 4: Rights override example 1

"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.

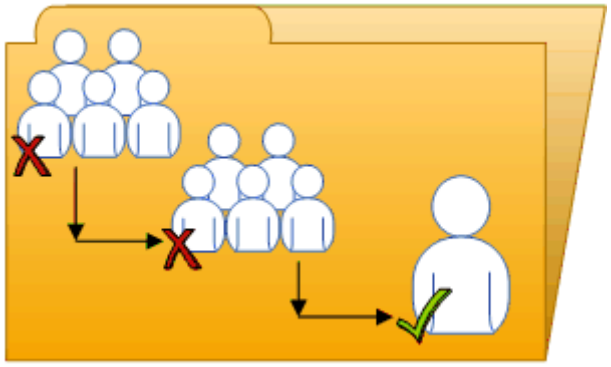


Figure 5: Rights override example 2

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

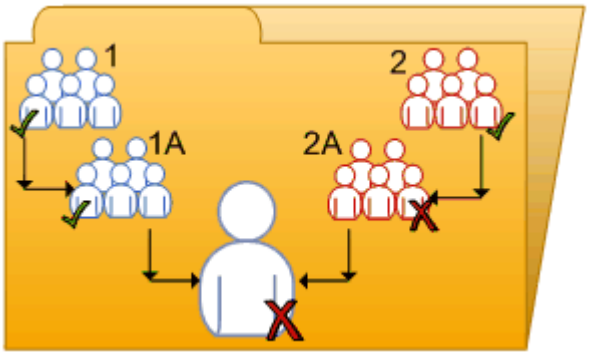


Figure 6: Complex rights override

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.

7.1.3.4 Scope of rights

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

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

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

7.1.4 Type-specific rights

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

- General rights for the object type

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

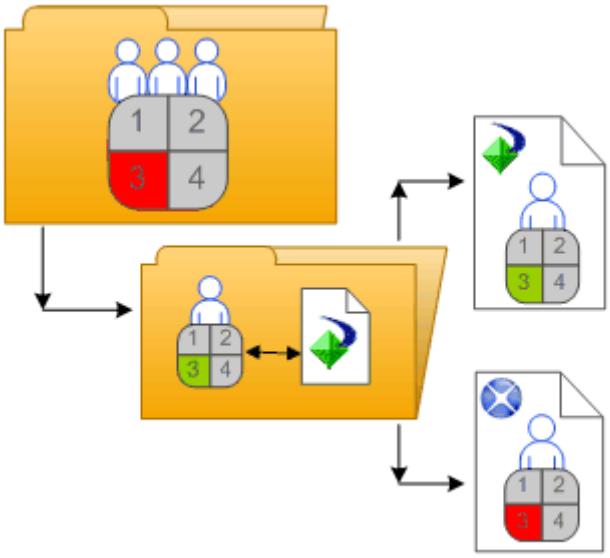


Figure 7: Type-specific rights example

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 BI platform application they affect. Examples of applications include the CMC and BI launch pad.
- *System*
  These rights are divided according to which core system component they affect. Examples of core system components include Calendars, Events, and Users and Groups.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

7.1.5 Determining effective rights

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

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

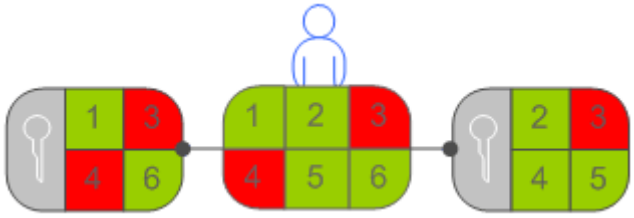


Figure 8: Multiple access levels

- 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.

7.2 Managing security settings for objects in the CMC

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

7.2.1 To view rights for a principal on an object

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.

7.2.2 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*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The *Add Principals* dialog box appears.

4. Move the users and groups you want to add as principals from the *Available users/groups* list to the *Selected users/groups* list.
5. Click *Add and Assign Security*.
6. Select the access levels you want to grant the principal.
7. Choose whether to enable or disable folder or group inheritance.

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

Related Information

To modify security for a principal on an object [page 122]

7.2.3 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 Information

To assign principals to an access control list for an object [page 121]

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

1. Go to the CMC area that has the top-level folder you want to set rights for.
2. Click *Manage* > *Top-Level Security* > *All* `<Objects>`.

   Here `<Objects>` represents the contents of the top-level folder. If you are prompted for confirmation, click *OK*.

   The *User Security* dialog box appears and displays the access control list for the top-level folder.
3. Assign the principal to the access control list for the top-level folder.
4. If necessary, assign advanced rights to the principal.

Related Information

To assign principals to an access control list for an object [page 121]
To modify security for a principal on an object [page 122]

7.2.5 Checking security settings for a principal

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

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

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

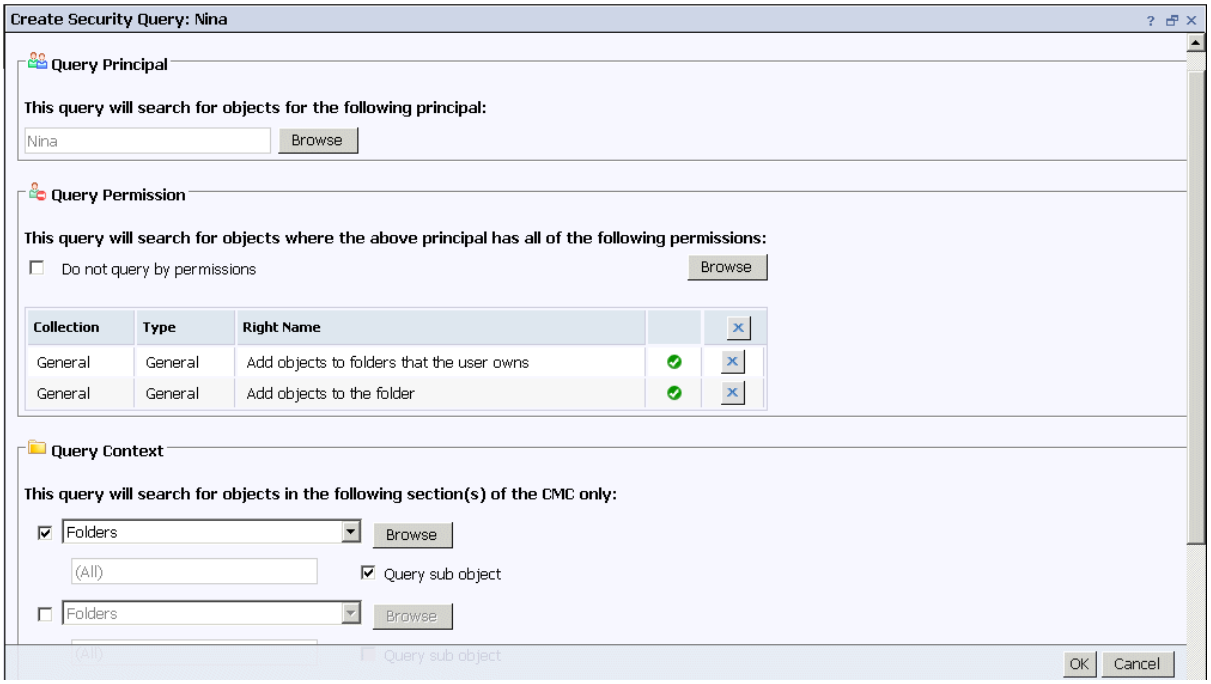
Security queries are useful because they allow you to see the objects that a principal has certain rights to, and they provide the locations of these objects if you want to modify those rights. Consider a situation in which a sales employee is promoted to sales manager. The sales manager needs *Schedule*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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

query. After the security query runs, the administrator can see all Crystal reports that the sales manager has *View* rights for in the *Query Results* area. Because the *Details* panel displays the location of each Crystal report, the administrator can browse for each report and modify the sales manager's rights on it.

7.2.5.1 To run a security query

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



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

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

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

   - If you want to run a general security query, select the *Do not query by permissions* check box.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

When you do this, the BI platform runs a general security query for all objects that have the principal in their access control lists regardless of the permissions that the principal has on the objects.

5. In the *Query Context* area, specify the CMC areas that you want to query.
   a. Select a check box next to a list.
   b. On the list, select a CMC area that you want to query.

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

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

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

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

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

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

7.3 Working with access levels

You can do the following with access levels:

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 13: Predefined access levels

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

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

Access level task	Rights required
Create an access level	*Add* right on the *Access Levels* top-level folder
View granular rights in an access level	*View* right on the access level
Assign an access level to a principal on an object	*View* right on the access level *Use the Access Level for Security Assignment* right on the access level *Modify Rights* right on the object, or *Securely Modify Rights* right on the object and the principal **Note** Users who have the *Securely Modify Rights* right and want to assign an access level to a principal must have that same access level assigned to themselves.
Modify an access level	*View* and *Edit* rights on the access level

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Access level task	Rights required
Delete an access level	*View* and *Delete* rights on the access level
Clone an access level	*View* right on the access level *Copy* right on the access level *Add* right on the *Access Levels* top-level folder

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

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

View On Demand access level

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

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

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

View access level

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

7.3.2 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.

7.3.3 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.

7.3.4 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.

7.3.5 To delete an access level

1. In the *Access Levels* area, in the *Details* panel, select the access level that you want to delete.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Click *Manage* > *Delete Access Level*.

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

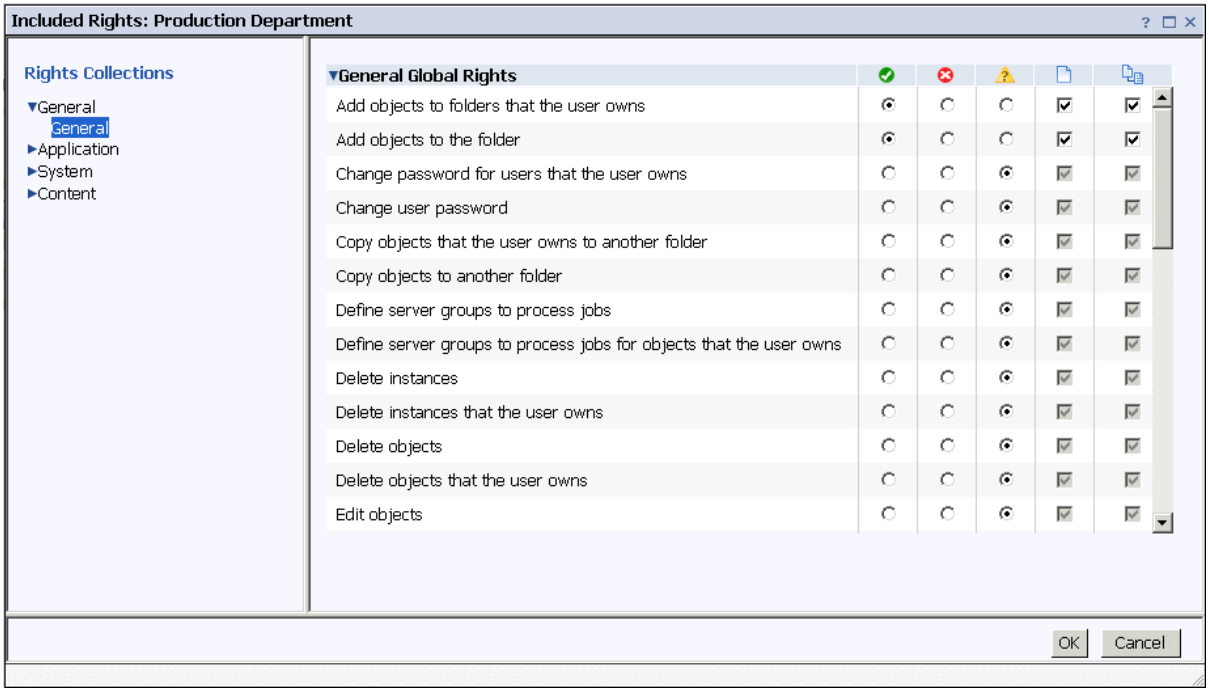
A dialog box appears with information about the objects that this access level affects. If you do not want to delete the access level, click *Cancel* to exit the dialog box.

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

7.3.6 To modify rights in an access level

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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. When you have finished, click *OK*.
   You return to the list of effective rights.

Related Information

Managing security settings for objects in the CMC [page 120]
Type-specific rights [page 118]

7.3.7 Tracing the relationship between access levels and objects

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

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

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

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

7.3.8 Managing access levels across sites

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

Modifying replicated access levels in the Origin site

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

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

Modifying replicated access levels in the Destination site

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

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

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

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

Related Information

Federation [page 690]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

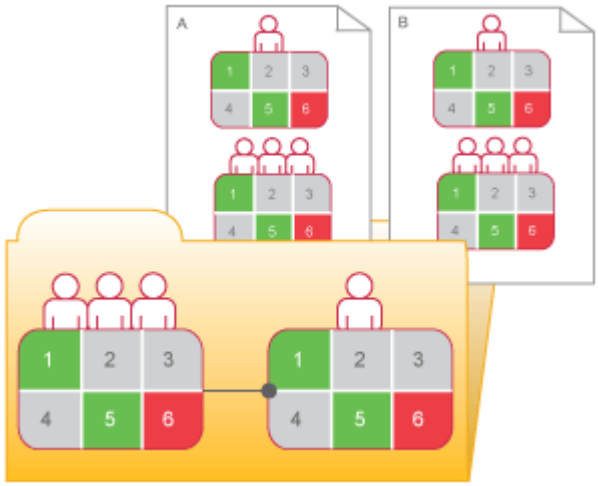
Tracing the relationship between access levels and objects [page 130]

7.4 Breaking inheritance

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

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

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



© 2015 SAP SE or an SAP affiliate company. All rights reserved.

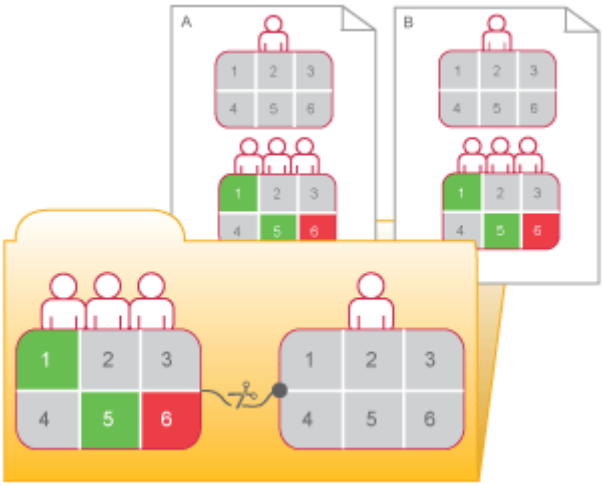


Figure 9: Breaking inheritance

7.4.1 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*.

7.5 Using rights to delegate administration

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

Table 14: Rights for delegated administrators

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

Modify the rights users have to objects

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

Securely modify the rights users have to objects

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Securely modify rights inheritance settings

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

7.5.2 Owner rights

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

Owner rights are useful in managing owner-based security. For example, you may want to create an folder or hierarchy of folders in which various users can create and view documents, but can only modify or delete their own documents. In addition, owner rights are useful for allowing users to manipulate instances of reports they create, but not others' instances. In the case of the scheduling access level, this permits users to edit, delete, pause and reschedule only their own instances.

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

7.6 Summary of recommendations for rights administration

Keep these considerations in mind for rights administration:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8 Securing the BI Platform

8.1 Security overview

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

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

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

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

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

8.2 Disaster recovery planning

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

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:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

8.3 General recommendations for securing your deployment

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

- Use firewalls to protect the communication between the CMS and other system components. If possible, always hide your CMS behind the firewall. At the very least, ensure that the system database is safely behind the firewall.
- Add additional encryption to the File Repository Servers. Once the system is up and running, proprietary content will be stored in these servers. Add additional encryption through the OS or use a third party tool.

  > **Note**
  >
  > The BI platform does not support SFTP. If you require SFTP functionality, please refer to SAP Note 1556571 or consider an SAP partner solution.

- Deploy a reverse proxy server in front of the web application servers in order to hide them behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, therefore hiding private IP addresses.
- Strictly enforce corporate password policies. Ensure that user passwords are routinely changed.
- If you have opted to install the system database and web application server provided with the BI platform, you should access the relevant documentation to ensure these components are deployed with adequate security configurations.
- Use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your deployment.
- Ensure that the platform installation directory and subdirectories are secured. Sensitive temporary data may be stored in these directories during system operation.
- Access to the Central Management Console (CMC) should be restricted to local access only. For information on deployment options for the CMC see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
- By default, Web Intelligence error messages include database schema information. To show error messages without the database schema information, perform the following steps:

  1. Open the `WebIContainer_ServerDescriptor.xml` configuration file for editing. By default, it is located at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\config`.
  2. Change the value of this parameter to False: `WebiParamDetailedDbErrorsEnabled = False`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Configuring the SSL protocol [page 160]
Password restrictions [page 144]
Configuring security for bundled third-party servers [page 139]

8.4 Configuring security for bundled third-party servers

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

- Sybase SQL Anywhere: For detailed information on securing this system database see http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.0/dbadmin/da-part-securing.html.
- Apache Tomcat: For detailed information on security for this web application server, see http://tomcat.apache.org/ .

8.5 Active trust relationship

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

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

8.5.1 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 the BI platform.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

8.5.2 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).

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

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

8.6 Sessions and session tracking

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

The BI platform uses two common methods to store session state:

- Cookies—A cookie is a small text file that stores session state on the client side: the user's web browser caches the cookie for later use. The BI platform logon token is an example of this method.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Session variables—A session variable is a portion of memory that stores session state on the server side. When the BI platform grants a user an active identity on the system, information such as the user's authentication type is stored in a session variable. So long as the session is maintained, the system neither has to prompt the user for the information a second time nor has to repeat any task that is necessary for the completion of the next request.
  For Java deployments, the session is used to handle .jsp requests; for .NET deployments, the session is used to handle .aspx requests.

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

8.6.1 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.

8.6.2 Managing sessions

You can view and terminate sessions in the CMC.

You can view and terminate user sessions in the Central Management Console (CMC). For example, you may want to see which users are using multiple sessions. Or, you may want to terminate sessions consuming too many system resources, or very old sessions. You might also need to terminate sessions when preparing for system downtime or upgrades.

8.6.2.1 To view the session list

View sessions in the CMC.

You can view a list of sessions in the Central Management Console.

1. Log in to the CMC as an administrator.
2. From the *Manage* area, click *Sessions*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The list of user sessions for the cluster is displayed. You can click the column headers to sort the list by user name, by the number of open sessions, or by logon times. You can also click the user name or session count or logon time to display details for that user's sessions in the lower pane.

8.6.2.2 To terminate sessions

Terminate sessions in the CMC.

You can terminate single or multiple sessions.

1. Log in to the CMC as an administrator.
2. From the *Manage* area, click *Sessions*.
   The list of user sessions for the cluster is displayed.
3. Click a user name or session count or logon time, to display a user's sessions in the lower pane.
4. Click to select a single session, or `CTRL` + `click` to select multiple sessions.
5. Click *End Session*.

> **Note**
>
> To terminate sessions, you must have the "Edit objects" right on the CMS object.

> **Note**
>
> You cannot terminate your current administrator session.

8.7 Environment protection

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

8.7.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

8.7.2 Web server to BI platform

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

8.8 Auditing security configuration modifications

Any changes to default security configurations for the following will not be audited by the BI platform:

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

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

8.9 Auditing web activity

The BI platform 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.

8.9.1 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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

process of simply guessing a valid user name and password remains a viable way to attempt to "crack" the system.

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

8.9.2 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.

8.9.3 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, the BI platform has an internal mechanism that enforces a time delay (0.5–1.0 second) between logon attempts. In addition, the platform provides several customizable options that you can use to reduce the risk of a dictionary attack:

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

8.9.4 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,

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

even if a malicious user does guess or otherwise obtain another user's credentials, they are valid only for a limited time.

8.9.5 Guest account restrictions

The BI platform supports anonymous single sign-on for the Guest account. Thus, when users connect to the BI platform without specifying a user name and password, the system logs them on automatically under the Guest account. If you assign a secure password to the Guest account, or if you disable the Guest account entirely, you disable this default behavior.

8.10 Processing extensions

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

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

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

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

8.11 Overview of BI platform data security

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

8.11.1 Data processing security modes

The BI platform can operate in two possible data processing security modes:

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

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

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

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

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

8.11.1.1 To turn on FIPS-compliant mode on Windows

By default, FIPS-compliant mode is turned off when the BI platform is installed. However, you can turn on FIPS compliancy for all nodes in your deployment.

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

   > **Caution**
   >
   > Do not proceed to step 3 until the SIA status is Stopped.

3. Right-click the SIA and select *Properties*.
   The *Properties* dialog box appears, displaying the *Properties* tab.
4. Add `-fips` to the *Command* field, and click *Apply*.
5. Click *OK* to close the *Properties* dialog box.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Restart the SIA.

The SIA is now operating in FIPS-complaint mode.

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

8.11.1.2 To turn on FIPS-compliant mode on UNIX

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

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

1. From the **<INSTALLDIR>**`/sap_bobj` directory, open the `ccm.config` file for editing.
2. Add `-fips` to the node launch command parameter.

   The node launch command parameter is displayed in this format: **<NODENAME>**`LAUNCH`. For example, for a node named "SAP", the node launch command parameter is `SAPLAUNCH`.
3. Save your changes and *Exit*.
4. Restart the node.

The node is now operating in FIPS-complaint mode.

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

8.11.1.3 To turn off FIPS-compliant mode on Windows

All servers in your BI platform 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 with the *Properties* tab displayed.
3. Remove `-fips` from the *Command* field and click *Apply*.
4. Click *OK* to close the *Properties* dialog box.
5. Restart the SIA.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.12 Cryptography in the BI platform

Sensitive Data

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

The BI platform system uses a two-key cryptography system.

Cryptographic Keys

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

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

Cluster Keys

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

8.12.1 Working with cluster keys

During the installation setup for the BI platform, an eight character cluster key is created for the Server Intelligence Agent. This key is used to encrypt all the cryptographic keys in the CMS repository. Without the correct cluster key you cannot access the CMS.

The cluster key is stored in encrypted format in a `dbinfo` file. The `dbinfo` filename follows this convention: `_boe_<sia_name>.dbinfo`, where `<sia_name>` is the name of the Server Intelligence Agent for the cluster.

On Windows, the file is stored in the following directory: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

On Unix systems, the file is stored in the platform directory under `<INSTALLDIR>/sap_bobj/enterprise_xi40/`:

Unix platform	Platform directory
AIX	`<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`

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

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

8.12.1.1 To reset the cluster key on Windows

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

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

   > **Caution**
   >
   > Do not proceed to step 3 until the SIA status is Stopped.

3. Right-click the Server Intelligence Agent (SIA) and select *Properties*.
   The *Properties* dialog box appears.
4. Click the *Configuration* tab.
5. Click *Change* under *CMS Cluster Key Configuration*.
   A warning message appears.
6. Click *Yes* to continue.
   The *Change Cluster Key* dialog box appears.
7. Enter the same eight-character key in the *New Cluster Key* and *Confirm New Cluster Key* fields.

   > **Note**
   >
   > On Windows, cluster keys must contain a combination of uppercase and lowercase characters. Alternately, users can also generate a random key. A random key is required in order to be FIPS-compliant.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

8.12.1.2 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. Navigate to the `<INSTALLDIR>/sap_bobj` directory.
2. Type **`./cmsdbsetup.sh`** and press *Enter*.
   The *CMS Database Setup* screen appears.
3. Type the name of the node and press *Enter*.
4. Type **2** to change the cluster key.
   A warning message appears.
5. Select *Yes* to continue.
6. In the field provided, type 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.

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

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

8.12.2 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 the BI platform is also a member of the Cryptographic Officers group. Use this account to add users to the Cryptographic Officers group as required. It is recommended that membership to the group be restricted to a limited number of users.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.12.2.1 To add a user to the Cryptographic Officers group

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

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

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

   > **Tip**
   >
   > To search for a specific user, use the search field.
5. Click *OK*.

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

8.12.2.2 To view cryptographic keys in the CMC

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

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

Related Information

To view objects associated with a cryptographic key [page 153]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.12.3 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 Status Change	Date and time stamp for the last change associated with the cryptographic key
Objects	Number of objects associated with the key

Related Information

Cryptographic key status [page 152]
To create a new cryptographic key [page 154]
To delete a cryptographic key from the system [page 155]
To revoke a cryptographic key [page 155]
To view objects associated with a cryptographic key [page 153]
To mark cryptographic keys as compromised [page 154]

8.12.3.1 Cryptographic key status

The following table lists all the possible status options for cryptographic keys in the BI platform:

Status	Description
Active	Only one cryptographic key can be designated *Active* in the system. This key is used to encrypt current sensitive data that will be stored in the CMS database. The key is also used to decrypt all the objects that appear in its Object List. Once a new cryptographic key is created, the current *Active* reverts to the *Deactivated* state. An active key cannot be deleted from the system.
Deactivated	A *Deactivated* key can no longer be used to encrypt data. It can however be used to decrypt all the objects that appear in its Object List. You cannot reactivate a key once it has been deactivated. A key marked as *Deactivated* cannot be deleted. from the system. You must change a key's status to *Revoked* before it can be deleted.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Status	Description
Compromised	A cryptographic key that is deemed to be insecure can be marked as compromised. By flagging such a key, you can later proceed to re-encrypt data objects that are still associated with the key. Once a key is marked as compromised it must be revoked before it can be deleted from the system.
Revoked	When a cryptographic key is revoked, a process is launched in which all objects currently associated with the key are re-encrypted with the current "Active" cryptographic key. Once a key is revoked it can safely be deleted from the system. The revocation mechanism ensures that data in the CMS database can always be decrypted. There is no way to reactivate a key once it has been revoked.
Deactivated: Rekeying-in process	Indicates that the cryptographic key is in the process of being revoked. Once the process is complete, the key will be marked as *Revoked*.
Deactivated: Rekeying-suspended	Indicates that the process for revoking a cryptographic key has been suspended. This usually occurs if the process has been deliberately suspended or if a data object associated with the key is not available.
Revoked-Compromised	A key is flagged as Revoked-Compromised if has been marked as compromised and all the data previously associated with it has been encrypted with another key. When a *Deactivated* key is marked as compromised, you are given a choice of not taking action or revoking the key. Once a compromised key is revoked it can be deleted.

8.12.3.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.12.3.3 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 appears.
2. Click *Continue* to create the new cryptographic key.
3. Type the name and a description of the new cryptographic key; click *OK* to save your information.
   The new key is listed as the only active key in the *Cryptographic Keys* management area. The previously *Active* key is now marked as *Deactivated.*

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

8.12.3.4 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 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 appears.
4. Click *Continue*.
5. Select one of following options from the *Mark As Compromised* dialog:
   - *Yes*: launches the process to re-encrypt all data objects that are associated with the compromised key.
   - *No*: the *Mark As Compromised* dialog box is closed and the cryptographic key is marked as *Compromised* in the *Cryptographic Keys* management area.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To revoke a cryptographic key [page 155]
Cryptographic key status [page 152]
To view objects associated with a cryptographic key [page 153]

8.12.3.5 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.

1. Select the key you want to revoke from the keys listed in the *Cryptographic Keys* management area.
2. Click *Actions* > *Revoke*.
   The *Revoke* dialog box appears.
3. Click *OK*.
   A process is launched to encrypt all the key's objects with the current active key. If the key is associated with many data objects, it will be marked as *Deactivated: Re-encryption in process* until the re-encryption process is complete.

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

8.12.3.6 To delete a cryptographic key from the system

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To revoke a cryptographic key [page 155]
Cryptographic key status [page 152]

8.13 Configuring servers for SSL

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

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

- Deploy the BI platform with SSL enabled.
- Create key and certificate files for each machine in your deployment.
- Configure the location of these files in the Central Configuration Manager (CCM) and your web application server.
- Or, configure SSL for certificates that are managed by a certificate authority.

> **Note**
>
> If you are using thick clients, such as Crystal Reports, 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.

8.13.1 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.

> **Note**
>
> For maximum security, all private keys should be protected and should not be transferred through unsecured communication channels.

> **Note**
>
> Certificates created for previous versions of the BI platform will not work for SAP BI platform 4.0. These certificates will need to be re-created.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.13.1.1 To create key and certificate files for a machine

1. Run the `sslc` command line tool.

   The SSLC tool is installed with your BI platform software. (On Windows, for example, it is installed by default in **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)
2. Enter 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, enter 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, enter 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. In a text editor, open the `sslc.cnf` file that is located in the same folder as the SSLC command line tool.

   > **Note**
   >
   > You must use a text editor for Windows because Windows Explorer may not recognize and display files with a `.cnf` extension.

6. Perform the following actions, based on settings in the `sslc.cnf` file:
   a. 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
      ```

   b. Create a file with the name specified by the `sslc.cnf` file's `database` setting.

      > **Note**
      >
      > By default, the file is called `$dir/index.txt` and should be empty.

   c. Create a file with the name specified by the `sslc.cnf` file's `serial` setting.

      This file must provide an octet-string serial number (in hexadecimal format).

      > **Note**
      >
      > To ensure that you can create and sign more certificates, choose a large hexadecimal number with an even number of digits, such as 11111111111111111111111111111111.

   d. Create the directory specified by the `sslc.cnf` file's `new_certs_dir` setting.
7. To create a certificate request and a private key, enter the following command:

   ```
   sslc req -config sslc.cnf -new -out servercert.req
   ```

   The certificate and key files generated are placed in the current working folder.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8. To decrypt the key in the `privkey.pem` file, enter the following command:

   ```
   sslc rsa -in privkey.pem -out server.key
   ```

9. To sign the certificate with the CA certificate, enter 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`) must be generated only once per deployment. All machines in the same deployment share the same CA certificates. All other certificates must be signed by the private key of any CA certificate.

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) that can be accessed by the machines in your BI platform deployment:
    - Trusted certificate file (`cacert.der`)
    - Generated server certificate file (`servercert.der`)
    - Server key file (`server.key`)
    - Passphrase file (`passphrase.txt`)

    This location will be used to configure SSL for the CCM and your web application server.

8.13.2 Setting up SSL when the certificate is managed by a certificate authority

When setting up SSL for server communication, follow these steps if the certificate is managed by a certificate authority.

1. Export your desired certificate with its private key to PKCS #12 (.PFX) format.

   This will be used as the certificate for the certificate authority.

2. Using OpenSSL, run the following commands:

   1. Export the private key file from the .pfx file:
      ```
      openssl pkcs12 -in filename.pfx -nocerts -out privkey.pem
      ```
   2. Export the certificate file from the .pfx file:
      ```
      openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cacert.pem
      ```
   3. Remove the passphrase from the private key:
      ```
      openssl rsa -in privkey.pem -out cakey.pem
      ```

3. Set up some required files:
   - Copy `cakey.pem` to `C:\SSL\private\cakey.pem`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Copy `cacert.pem` to `C:\SSL\cacert.pem`.
- Create an empty text file (a database index file) named `index.txt` in the `C:\SSL` folder.
- Create another text file: `C:\SSL\serial`.
- Open the `C:\SSL\serial` file in a text editor, type the following value, and save the file: `1111111111111111111`

4. In a text editor, open the file `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\sslc.cnf`.

   Choose one of these options:

   - Change the value of the `policy` variable to `policy_anything`. This change lets you create a server certificate that doesn't have the same policies as your certificate authority certificate.
   - Or, keep the value of the `policy` variable unchanged as `policy_match`. This forces your server certificate to have the same policies as your certificate authority certificate. In this case, you may need to change the `req_distinguished_name` properties accordingly.

5. Create a certificate request and private key.

   In a command prompt, run the following command:

   ```
   sslc req -config sslc.cnf -new -out servercert.req
   ```

   > **Note**
   >
   > For the `PEM pass phrase`, type any password, using a minimum of four characters.

   > **Note**
   >
   > For the `Common Name`, type the fully qualified domain name of the machine where BI platform servers are running.

   > **Note**
   >
   > The file `servercert.req` is created in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

   > **Note**
   >
   > The files `.rnd` and `privkey.pem` are modified.

6. Decrypt the private key.

   ```
   sslc rsa -in privkey.pem -out server.key
   ```

7. Sign the certificate.

   ```
   sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
   ```

   > **Note**
   >
   > The file `servercert.pem` is created in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The file `1111111111111111111.pem` is created in `C:\SSL\newcerts`.

> **Note**
>
> A backup of the file `serial` is created, named `serial.old`.

> **Note**
>
> The value of `serial` is incremented from `11111111111111111111` to `11111111111111111112`.

8. Convert the certificates to DER encoding.

   Run these commands:

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

> **Note**
>
> The file `servercert.der` is created in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

> **Note**
>
> The file `cacert.der` is created in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

9. Create a text file named `passphrase.txt`.

   The content of the file should be the PEM pass phrase you used earlier.

10. Store the following files in a secure location; for example, `C:\SSLCerts`.
    - the trusted certificate file `cacert.der`
    - the generated server certificate file `servercert.der`
    - the server key file `server.key`
    - the passphrase file `passphrase.txt`

8.13.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.13.3.1 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: `d:\ssl`
Server SSL Certificate File	Name of the file used to store the server SSL certificate. By default, `servercert.der`
SSL Trusted Certificates File	Name of the file with the SSL trusted certificate. By default, `cacert.der`
SSL Private Key File	Name of the SSL private key file used to access the certificate. By default, `server.key`
SSL Private Key Passphrase File	Name of the text file containing the passphrase used to access the private key. By default, `passphrase.txt`

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

8.13.3.2 To configure the SSL protocol on Unix

You must use the `serverconfig.sh` script to configure the SSL protocol for a SIA. This script provides a text-based program that enables you to view server information and to add and delete servers from your installation. The `serverconfig.sh` script is installed on the `sap_bobj` directory in your installation.

1. Use the `ccm.sh` script to stop the SIA and all SAP BusinessObjects servers.
2. Run the `serverconfig.sh` script.
3. Select *3 - Modify Node*, and press `Enter`.
4. Specify the target SIA, and press `Enter`.
5. Select *1 - Modify Server Intelligence Agent SSL configuration*.
6. Select *ssl*.
   When prompted, specify the SSL certificate locations.
7. Repeat steps 1-6 for each SIA, if your BI platform deployment is a SIA cluster.
8. Start the SIA with the `ccm.sh` script, and wait for the servers to start.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.13.3.3 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:

   Table 15:

Example	Description
<DcertDir> =d:\ssl	The directory to store all the certificates and keys.
<DtrustedCert> =cacert.der	Trusted certificate file. If specifying more than one, separate with semicolons.
<DsslCert> =clientcert.der	Certificate used by the SDK.
<DsslKey> =client.key	Private key of the SDK certificate.
<Dpassphrase> =passphrase.txt	The file that stores the passphrase for the private key.

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

8.13.3.4 To configure thick clients

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	**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 thick client applications such as the Central Configuration Manager (CCM) or the upgrade management tool.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

3. Type the following command:

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

4. Restart the thick client application.

Related Information

To create key and certificate files for a machine [page 157]

8.13.3.4.1 To configure SSL login for the 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.oci.protocol=ssl -DcertDir=<D:\SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Save the file and close the text editor.

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

8.13.3.4.2 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 BI platform deployment.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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. Locate the following line:

   ```
   start "" "%JRE%\bin\javaw" -cp migration.jar;*  -Xmx512m -Xss10m
   com.bo.migration.MigrationTool
   ```

4. Add the following after the -Xss10m parameter:

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

   > **Note**
   >
   > Ensure there is a space between each parameter, and no spaces at the ends of the lines.

5. Save the file and close the text editor.

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

Related Information

To create key and certificate files for a machine [page 157]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.14 Understanding communication between BI platform components

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

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

Related Information

Configuring the BI platform for firewalls [page 172]
Examples of typical firewall scenarios [page 177]

8.14.1 Overview of BI platform servers and communication ports

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

8.14.1.1 Each BI platform server binds to a request port

A BI platform server, the Input File Repository Server for example, binds to a request port when it starts. Other BI platform components including servers, rich clients, and the SDK hosted in the web application server can use this request port to communicate with the server.

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

8.14.1.2 Each BI platform server registers with the CMS

BI platform servers register with the CMS when they start. When a server registers, the CMS records:

- The hostname (or IP address) of the server's host machine.
- The server's Request Port number.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.14.1.3 The CMS uses two ports

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

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

8.14.1.4 Central Management Server (CMS) directory of registered services

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

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

> **Note**
>
> The reference to a BI platform server will contain the server machine's host name by default. (If a machine has more than one host name, the primary host name is chosen). You can configure a server so that its reference contains the IP address instead.

Related Information

Communication between BI platform components [page 167]

8.14.1.5 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.14.1.6 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 creates one or more child processes. Each child process has its own Request Port.

By default, a job server will dynamically select a Request Port for each child process. You can specify a range of port numbers that the job server can select from.

All child processes communicate with the CMS. If this communication crosses a firewall, you must:

- Specify the range of port numbers that the job server can select from by adding the `-requestJSChildPorts <lowestport>-<highestport>` and `-requestPort <port>` parameters to the server's command line. Note that the port range should be large enough to allow the maximum number of child process as specified by `-maxJobs`.
- Open the specified port range on the firewall.

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

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

Related Information

Command lines overview [page 817]

8.14.2 Communication between BI platform components

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

8.14.2.1 Requirements for communication between BI platform components

Deployments of the BI platform must conform to these general requirements.

1. Every server must be able to initiate communication with every other BI platform server on that server's Request Port.
2. The Central Management Server uses two ports. Every BI platform server, rich client, and the web application server that hosts the SDK must be able to initiate communication with the CMS on both of its ports.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Every job server child process must be able to communicate with the CMS.
4. Thick clients must be able to initiate communication with the Request Port of the Input and Output File Repository Servers.
5. If auditing is enabled for thick clients and web applications, they must be able to initiate communication with the request ports of the Adaptive Processing Servers that host the Client Auditing Proxy Service.
6. In general, the web application server that hosts the SDK must be able to communicate with the Request Port of every BI platform server.

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

7. Job Servers use the port numbers that are specified with the `-requestJSChildPorts <lowestport>-<highestport>` command. If no range is specified in the command line, the servers use random port numbers. To allow a job server to communicate with a CMS, FTP, or mail server on another machine open all of the ports in the range specified by `-requestJSChildPorts` on your firewall.
8. The CMS must be able to communicate with the CMS database listen port.
9. The Connection Server, most Job Server child process, and every system database and auditing Processing Server must be able to initiate communication with the reporting database listen port.

Related Information

BI platform port requirements [page 168]

8.14.2.2 BI platform port requirements

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

8.14.2.2.1 Port Requirements for BI platform applications

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 16:

Product	Client Application	Associated Servers	Server Port Requirements
Crystal Reports	SAP Crystal Reports 2013 designer	CMS Input FRS Output FRS Crystal Reports 2013 Report Application Server (RAS) Crystal Reports 2013 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 2013 Report Application Server Request Port Crystal Reports 2013 Processing Server Request Port Crystal Reports Cache Server Request Port
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 (`dswsbobje.war`) 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 (`dswsbobje.war`) that hosts the Live Office web service	HTTP port (80 by default)
BI platform	SAP BusinessObjects Web Intelligence Rich Client	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Product	Client Application	Associated Servers	Server Port Requirements
BI platform	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
BI platform	Business View Manager	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port
BI platform	Central Configuration Manager (CCM)	CMS Server Intelligence Agent (SIA)	The following ports must be open to allow CCM to manage remote BI platform servers: CMS Name Server Port (6400 by default) CMS Request Port The following ports must be open to allow CCM to manage remote SIA processes: Microsoft Directory Services (TCP port 445) NetBIOS Session Service (TCP port 139) NetBIOS Datagram Service (UDP port 138) NetBIOS Name Service (UDP port 137) DNS (TCP/UDP port 53) (Note that some ports listed above may not be required. Consult your Windows administrator).
BI platform	Server Intelligence Agent (SIA)	Every BI platform server including the CMS	SIA Request Port (6410 by default) CMS Name Server Port (6400 by default) CMS Request Port
BI platform	Report Conversion Tool	CMS Input FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port
BI platform	Repository Diagnostic Tool	CMS Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Input FRS Request Port Output FRS Request Port

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Product	Client Application	Associated Servers	Server Port Requirements
BI platform	BI platform SDK hosted in the web application server	All BI platform servers required by the deployed products. For example, communication with the Crystal Reports 2013 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 2013 Processing Server Request Port.
BI platform	Web Services provider (`dswsbobje.war`)	All BI platform servers required by the products accessing the web services. For example, communication with the Dashboards Cache and Processing Server Request Ports is required if SAP BusinessObjects Dashboards is accessing Enterprise data source connections through the Web Services provider.	CMS Name Server Port (6400 by default) CMS Request Port Request Port for each server that is required. For example, the Dashboards Cache Server and Dashboards Processing Server Request Ports.
BI platform	SAP BusinessObjects Analysis, edition for OLAP	CMS Adaptive Processing Server hosting the Multi-Dimensional Analysis Service Input FRS Output FRS	CMS Name Server Port (6400 by default) CMS Request Port Adaptive Processing Server Request Port Input FRS Request Port Output FRS Request Port

8.14.2.2.2 Port Requirements for Third-Party Applications

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

Table 17:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Third-party application	SAP BusinessObjects 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 BusinessObjects web services and web applications including BI launch pad and CMC	HTTP port and HTTPS port. For example, on Tomcat the default HTTP port is 8080 and the default HTTPS port is 443.	The HTTPS port is only required if secure HTTP communication is used.
FTP server	Every Job Server	FTP In (port 21) FTP Out (port 22)	The Job Servers use the FTP ports to allow *send to FTP*.
Email server	Every Job Server	SMTP (port 25)	The Job Servers use the SMTP port to allow *send to email*.
Unix servers to which the Job Servers can send content	Every Job Server	rexec out (port 512) (Unix only) rsh out (port 514)	(Unix only) The Job Servers use these ports to allow *send to disk*.
Authentication Server	CMS™ web application server that hosts the SDK every thick Client, for example Live Office.	Connection port for third-party authentication. For example, the connection server for the Oracle LDAP server is defined by the user in the file ldap.ora.	User credentials are stored in the third-party authentication server. The CMS™, SDK, and the thick clients listed here need to communicate with the third-party authentication server when a user logs on.

8.15 Configuring the BI platform for firewalls

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.15.1 To configure the system for firewalls

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

Related Information

Communication between BI platform components [page 167]
Configuring port numbers [page 363]
Command lines overview [page 817]
Specifying the firewall rules [page 173]
Configure the hosts file for firewalls that use NAT [page 174]

8.15.1.1 Specifying the firewall rules

You must configure the firewall to allow the necessary traffic between BI platform components. Consult your firewall documentation for details of how to specify these rules.

Specify one inbound access rule for each communication path that crosses the firewall. You might not need to specify an access rule for every BI platform server behind the firewall.

Use the port number you specify in the server *Request Port* box on the server's Properties page in the CMC. Remember that each server on a machine must use a unique port number. Some SAP BusinessObjects servers use more than one port.

> **Note**
>
> If the BI platform is deployed across firewalls that use NAT, every server on all machines needs a unique Request Port number. That is, no two servers in the entire deployment can share the same Request Port.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Example

This example shows the inbound access rules for a firewall between the web application server and the BI platform servers. In this case you would open two ports for the CMS, one port for the Input File Repository Server (FRS), and one port for the Output FRS. The Request Port numbers are the port numbers you specify in the *Request Port* box on the CMC configuration page for a server.

Table 18:

Source Computer	Port	Destination Computer	Port	Action
web application server	Any	CMS	6400	Allow
web application server	Any	CMS	<Request Port number>	Allow
web application server	Any	Input FRS	<Request Port number>	Allow
web application server	Any	Output FRS	<Request Port number>	Allow
Any	Any	CMS	Any	Reject
Any	Any	Other platform servers	Any	Reject

Related Information

Communication between BI platform components [page 167]

8.15.1.2 Configure the hosts file for firewalls that use NAT

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

Note

The BI platform can be deployed on machines that use Domain Name System (DNS). In this case, the server machine host names can be mapped to externally routable IP address on the DNS server, instead of in each machine's `hosts` file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Understanding Network Address Translation

A firewall is deployed to protect an internal network from unauthorized access. Firewalls that use *NAT* will map the IP addresses from the internal network to a different address that is used by the external network. This *address translation* improves security by hiding the internal IP addresses from the external network.

BI platform components such as servers, thick clients, and the web application server hosting the SDK will use a service reference to contact a server. The service reference contains the hostname of the server's machine. This hostname must be routable from the BI platform component's machine. This means the `hosts` file on the component's machine must map the server machine's hostname to the server machine's external IP address. The server machine's external IP address is routable from external side of the firewall, whereas the internal IP address is not.

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

8.15.1.2.1 To configure the hosts file on Windows

1. Locate every machine that runs a BI platform component that must communicate across a firewall on which *Network Address Translation* (*NAT*) is enabled.
2. On each machine located in the previous step, open the `hosts` file using a text editor like Notepad. The `hosts` file is located at `\Windows\System32\drivers\etc\hosts`.
3. Follow the instructions in the `hosts` file to add an entry for each machine behind the firewall that is running a BI platform server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

8.15.1.2.2 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 a BI platform component that must communicate across a firewall on which *Network Address Translation* (*NAT*) is enabled.
2. Open the *hosts* file using an editor like `vi`. The `hosts` file is located in the following directory `\etc`
3. Follow the instructions in the `hosts` file to add an entry for each machine behind the firewall that is running a BI platform server or servers. Map the server machine's hostname or fully qualified domain name to its external IP address.
4. Save the `hosts` file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.15.2 Debugging a firewalled deployment

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

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

- *Server* - The name of the server and whether it successfully started.
- *Published Address(es)* - A list of IP Address and port combinations which are posted to the name service that other servers will use to communicate with this server.

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

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

Note

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

Example

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

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

8.15.2.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

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

Related Information

Configuring port numbers [page 363]

8.16 Examples of typical firewall scenarios

This section provides examples of typical firewall deployment scenarios.

8.16.1 Example - Application tier deployed on a separate network

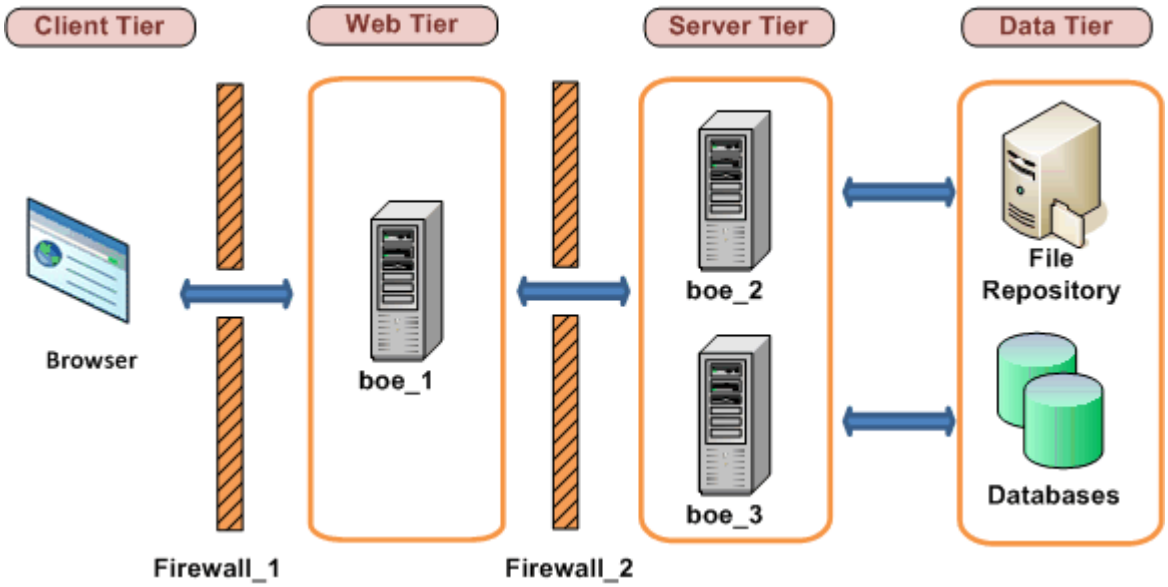
This example shows how to configure a firewall and the BI platform to work together in a deployment where the firewall separates the web application server from other BI platform servers.

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

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

Figure 10: Application tier deployed on a separate network

© 2015 SAP SE or an SAP affiliate company. All rights reserved.



8.16.1.1 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 SDK must be able to communicate with the CMS on both of its ports.
   - The web application server that hosts the SDK must be able to communicate with every BI platform server.
   - The browser must have access to the http or the https Request Port on the Web Application Server.
2. The web application server must communicate with all BI platform servers on machine `boe_2` and `boe_3`. Configure the port numbers for each server on these machines. Note that you can use any free port between 1,025 and 65,535.
   The port numbers chosen for this example are listed in the table:

   Table 19:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Server	Port Number
Web Intelligence Processing Server	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. Configure the firewalls `Firewall_1` and `Firewall_2` to allow communication to the fixed ports on the servers and the web application server that you configured in the previous step.

   In this example we are opening the HTTP Port for the Tomcat Application server.

   Table 20: Configuration for Firewall_1

Port	Destination Computer	Port	Action
Any	boe_1	8080	Allow

   Table 21: 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

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

Related Information

Configuring port numbers [page 363]
Understanding communication between BI platform components [page 165]

8.16.2 Example - Thick client and database tier separated from BI platform servers by a firewall

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

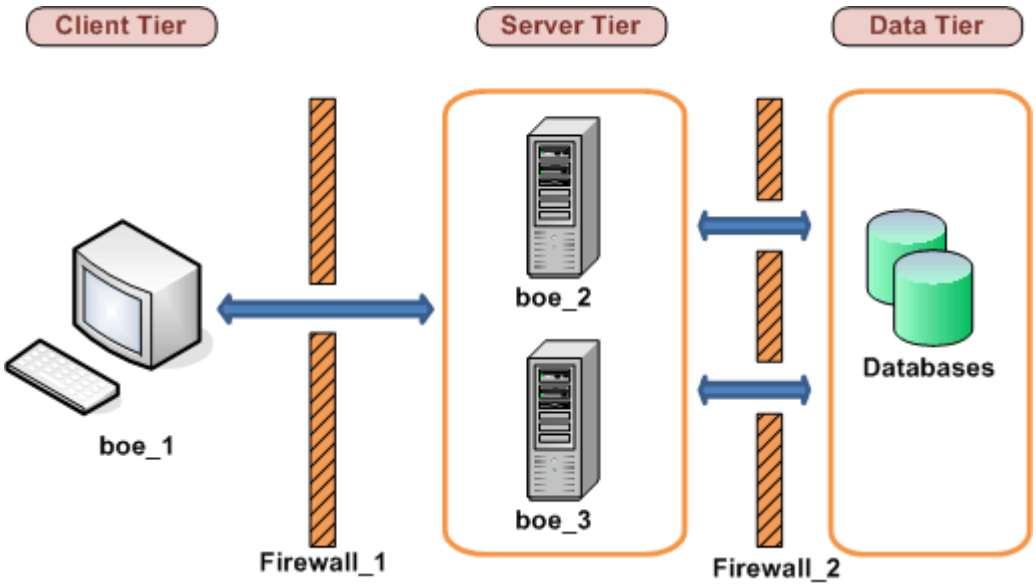
© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- One firewall separates a thick client from the BI platform servers.
- One firewall separates the BI platform servers from the database tier.

In this example, the BI platform components are deployed across these machines:

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

Figure 11: Rich client and database tier deployed on separate networks



8.16.2.1 To configure tiers separated from BI platform 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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:

   Table 22:

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 platform servers that you configured in the previous step. Note that port 6400 is the default port number for the CMS™ Name Server Port and did not need to be explicitly configured in the previous step.

   Table 23:

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.

   Table 24:

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

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

Related Information

Understanding communication between BI platform components [page 165]
Configuring the BI platform for firewalls [page 172]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.17 Firewall settings for integrated environments

This section details specific considerations and port settings for BI platform deployments that integrate with the following ERP environments.

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

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

Port requirements for BI platform servers

The following ports are required for their corresponding servers in the BI platform:

Table 25:

Server Port Requirements
• Central Management Server Name Server port • Central Management Server Request port • Input FRS Request port • Output FRS Request port • Report Application Server Request port • Crystal Reports Cache Server Request port • Crystal Reports Page Server Request port • Crystal Reports Processing Server Request Port

8.17.1 Specific firewall guidelines for SAP integration

Your BI platform deployment must conform to the following communication rules:

- The CMS must be able to initiate communication with SAP system on SAP System Gateway port.
- The Adaptive Job Server and Crystal Reports Processing Server (along with Data Access components) must be able to initiate communication with SAP system on the SAP System Gateway port.
- The BW Publisher component must be able to initiate communication with the SAP system on the SAP System Gateway port.
- BI platform components deployed on the SAP Enterprise Portal side (for example, iViews and KMC) must be able to initiate communication with BI platform web applications on HTTP/HTTPS ports.
- The web application server must be able to initiate communication on the SAP System Gateway service.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Crystal Reports must be able to initiate communication with the SAP host on the SAP System Gateway port and SAP System Dispatcher port.

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

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

Related Information

Installing a local SAP Gateway [page 737]

8.17.1.1 Detailed port requirements

Port requirements for SAP

The BI platform 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	BI platform Web Application Server	Web Service HTTP/ HTTPS port	Allow
SAP	Any	CMS	CMS Name Server port	Allow
SAP	Any	CMS	CMS Requested port	Allow
Web Application Server	Any	SAP	SAP System Gateway Service port	Allow
Central Management Server (CMS)	Any	SAP	SAP System Gateway Service port	Allow
Crystal Reports™	Any	SAP	SAP System Gateway Service port and SAP System Dispatcher port	Allow

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.17.2 Firewall configuration for JD Edwards EnterpriseOne integration

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

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

Port Requirements for BI platform servers

Table 26:

Product	Server Port Requirements
SAP BusinessObjects Business Intelligence platform	• BI platform Sign-on Server port

Port Requirements for JD Edwards EnterpriseOne

Table 27:

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

Configuring the web application server to communicate with JD Edwards

This section shows how to configure a firewall and the BI platform to work together in a deployment scenario where the firewall separates the web application server from other platform servers.

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 28: For JD Edwards EnterpriseOne Enterprise

Source Computer	Port	Destination Computer	Port	Action
CMS with Security Connectivity feature for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
BI platform servers with Data Connectivity for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
Crystal Reports with client side Data Connectivity for JD Edwards EnterpriseOne	Any	JD Edwards EnterpriseOne	Any	Allow
Web application server	Any	JD Edwards EnterpriseOne	Any	Allow

8.17.3 Specific firewall guidelines for Oracle EBS

Your deployment of the BI platform must allow the following components to initiate communication with the Oracle database listener port:

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

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

8.17.3.1 Detailed port requirements

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

Table 29:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.17.4 Firewall configuration for PeopleSoft Enterprise integration

Deployments of the BI platform that will communicate with PeopleSoft enterprise must conform to the following general communication rules:

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

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

Port Requirements for BI platform servers

Table 30:

Product	Server Port Requirements
SAP BI platform	• BI platform Sign-on Server port

Port Requirements for PeopleSoft

Table 31:

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

Configuring BI platform and PeopleSoft for firewalls

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

For firewall configuration with BI platform servers and clients, refer to the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

Besides the firewall configuration with the BI platform, you will need to do some extra configuration.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 32: For PeopleSoft Enterprise: PeopleTools 8.46 or newer

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

8.17.5 Firewall configuration for Siebel integration

This section shows which specific ports are used for communication between the BI platform and Siebel eBusiness Application systems when they are separated by firewalls.

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

Detailed description of ports

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 33: Port Requirements for BI platform servers

Product	Server Port Requirements
SAP BI platform	• BI platform Sign-on Server port

Table 34: Port Requirement for Siebel

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

Configuring BI platform firewalls for integration with Siebel

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

Table 35:

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

8.18 The BI platform and reverse proxy servers

The BI platform can be deployed in an environment with one or more reverse proxy servers. A reverse proxy server is typically deployed in front of the web application servers in order to hide them behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, hiding private IP addresses.

Because the reverse proxy server translates the public URLs to internal URLs, it must be configured with the URLs of the BI platform web applications that are deployed on the internal network.

8.18.1 Supported reverse proxy servers

The BI platform supports the following reverse proxy servers:

- IBM Tivoli Access Manager WebSEAL 6

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Apache 2.2
- Microsoft ISA 2006

8.18.2 Understanding how web applications are deployed

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

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps
```

WDeploy is used to deploy WAR files such as these:

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

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

8.19 Configuring reverse proxy servers for BI platform web applications

The reverse proxy server must be configured to map incoming URL requests to the correct web application in deployments where BI platform web applications are deployed behind a reverse proxy server.

This section contains specific configuration examples for some of the supported reverse proxy servers. Refer to the vendor documentation for your reverse proxy server for more information.

8.19.1 Detailed instructions for configuring reverse proxy servers

Configure the WAR files

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Specify BOE properties in the custom configuration directory

The `BOE.war` file includes global and application specific properties. If you need to modify the properties, use the custom configuration directory. By default the directory is located at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Caution

To avoid overwriting files in the default directory, do not modify the properties in the `config\default` directory. Users should use the `custom` directory.

Note

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

Consistent use of forward slashes (/)

Define the context paths in the reverse proxy server in the same way as they are entered in a browser URL. For example, if the directive contains a forward slash (/) at the end of the mirror path on the reverse proxy server, enter a forward slash at the end of the browser URL.

Ensure the '/' character is used consistently in the source and destination URL in the directive of the reverse proxy server. If the '/' character is added at the end of the source URL, it must also be added to the end of the destination URL.

8.19.2 To configure the reverse proxy server

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.19.3 To configure Apache 2.2 reverse proxy server for the BI platform

This section provides a workflow for configuring the BI platform and Apache 2.2 to work together.

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

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.19.4 To configure WebSEAL 6.0 reverse proxy server for the BI platform

This section explains how to configure the BI platform and WebSEAL 6.0 to work together.

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

1. Ensure that the BI platform and WebSEAL 6.0 are installed on separate machines.

   It is possible but not recommended to deploy the BI platform and WebSEAL 6.0 on the same machine. Refer to the WebSEAL 6.0 vendor documentation for instructions on configuring this deployment scenario.
2. Ensure that WebSEAL 6.0 is installed and configured as described in the vendor documentation.
3. Launch the WebSEAL *pdadmin* command line utility. Log in to a secure domain such as *sec_master* as a user with administration privileges.
4. Enter the following command at the *pdadmin sec_master* prompt:

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

   Where:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- `<port>` specifies the TCP port of the internal server that will receive the requests.
- `<junction_point>` specifies the directory in the WebSEAL protected object space where the document space of the internal server is mounted.

Example

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

8.19.5 To configure Microsoft ISA 2006 for the BI platform

This section explains how to configure the BI platform and ISA 2006 to work together.

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

1. Ensure that the BI platform and ISA 2006 are installed on separate machines.

   It is possible but not recommended to deploy the BI platform and ISA 2006 on the same machine. Refer to the ISA 2006 documentation for instructions on configuring this deployment scenario.
2. Ensure that ISA 2006 is installed and configured as described in the vendor documentation.
3. Launch the ISA Server Management utility.
4. Use the navigation panel to launch a new publishing rule
   a. Go to

      Arrays > *MachineName* > *Firewall Policy* > *New* > *Web Site Publishing Rule*

      Remember

      Replace `MachineName` with the name of the machine on which ISA 2006 is installed.

   b. Type a rule name in *Web publishing rule name* and click *Next*
   c. Select *Allow* as the rule action and click *Next*.
   d. Select *Publish a single Web site or load balancer* as the publishing type and click *Next*.
   e. Select a connection type between the ISA Server and the published Web site and click *Next*.

      For example, select *Use non-secured connections to connect the published Web server or server farm*.
   f. Type the internal name of the Web site you are publishing (for example, the machine name hosting BI platform) in *Internal site name* and click *Next*.

      Note

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. Click *New* to launch the New Web Listener Definition Wizard.
   a. Type a name in *Web listener name* and click *Next*.
   b. Select a connection type between the ISA Server and the published Web site and click *Next*.
      For example, select *Do not require SSL secured connections with clients*.
   c. In *Web Listener IP Addresses* section select the following and click *Next*.
      - Internal
      - External
      - Local Host
      - All Networks

      ISA Server is now configured to publish only over HTTP.
   d. Select an *Authentication Setting* option, click *Next*, and then click *Finish*.
      The new listener is now configured for the web publishing rule.
6. Click *Next* in *User Sets*, then click *Finish.*
7. Click *Apply* to save all the settings for the web publishing rule and update the ISA 2006 configuration.
   You now have to update the properties of the web publishing rule to map paths for the web applications.
8. In the navigation panel, right-click the Firewall Policy you configured and select *Properties*.
9. On the *Paths* tab, click *Add* to map routes to SAP BusinessObjects web applications.
10. On the *Public Name* tab, select *Request for the following Web sites* and click *Add*.
11. In the *Public Name* dialog box, type your ISA 2006 server name and click *OK*.
12. Click *Apply* to save all the settings for the web publishing rule and update the ISA 2006 configuration.
13. Verify the connections by accessing the following URL:

    `http://<ISA Server host Name>:<web listener port number>/<External path of the application>`

    For example: **`http://myISAserver:80/Product/BOE/CMC`**

    > **Note**
    >
    > You may have to refresh the browser several times.

You need to modify the HTTP policy for the rule have just configured to ensure that you will be able to logon on to the CMC. Right-click the rule you created in the ISA Server Management utility and select *Configure HTTP*. You must now deselect *Verify Normalization* in the *URL Protection* area.

To remotely access the BI platform you need to create an access rule.

8.20 Special configuration for the BI platform in reverse proxy deployments

Some BI platform products need additional configuration to function correctly in reverse proxy deployments. This section explains how to perform the additional configuration.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.20.1 Enabling reverse proxy for web services

This section describes the required procedures to enable reverse proxies for web services.

8.20.1.1 To enable reverse proxy on Tomcat

To enable reverse proxy on the Tomcat web application server, you must modify the `server.xml` file. Required modifications include setting `proxyPort` as the reverse proxy server listen port and adding a new `proxyName`. This section explains the procedure.

1. Stop Tomcat.
2. Open the `server.xml` for Tomcat.

   On Windows, `server.xml` is located at: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

   On Unix `server.xml` is located at `<CATALINA_HOME>/conf`. The default value of `<CATALINA_HOME>` is `<INSTALLDIR>/sap_bobj/tomcat`.
3. Locate this section in the server.xml file:

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!--See proxy documentation for more information about using
                this.-->
<!--
    <Connector port="8082"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
                enableLookups="false"
    acceptCount="100" debug="0" connectionTimeout="20000"
                proxyPort="80" disableUploadTimeout="true" />
    -->
```

4. Uncomment the Connector element by removing `<!--` and `-->`.
5. Modify the value of `proxyPort` to be the reverse proxy server listen port.
6. Add a new `proxyName` attribute to the Connector's attribute list. The value of the `proxyName` must be the proxy server name which should be resolvable to the correct IP address by Tomcat.

   Example:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
                <!--See proxy documentation for more information about using
                  this.-->
                <Connector port="8082"
                maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                enableLookups="false"
                acceptCount="100" debug="0"
connectionTimeout="20000"
                proxyName="my_reverse_proxy_server.domain.com"
                proxyPort="ReverseProxyServerPort"
                disableUploadTimeout="true" />
```

   Where `my_reverse_proxy_server.domain.com` and `ReverseProxyServerPort` should be substituted by the correct reverse proxy server name and its listen port.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

7. Save and close the `server.xml` file.
8. Restart Tomcat.
9. Ensure the reverse proxy server maps its virtual path to the correct Tomcat connector port. In the above example, the port is 8082.

   The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy SAP BusinessObjects™ Web Services deployed on Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
                ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

To enable web services, the proxy name and port number have to be identified for the connector.

8.20.1.2 Enabling reverse proxy for web services on web application servers other than Tomcat

The following procedure requires that BI platform web applications are successfully configured against your chosen web application server. Note that the `wsresources` are case-sensitive.

1. Stop the web application server.
2. Specify the external URL of the Web Services in the `dsws.properties` file.

   This file is located in `dswsbobje` web application. For example, if your external is URL is `http://my_reverse_proxy_server.domain.com/dswsbobje/`, update the properties in the dsws.properties file:

   - `wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine`
   - `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
   - `wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish`
   - `wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService`
   - `wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BIPlatform`
   - `wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/LiveOffice`
3. Save and close the `dsws.properties` file.
4. Restart the web application server.
5. Ensure the reverse proxy server maps its virtual path to the correct web application server connector port. The following example shows a sample configuration for Apache HTTP Server 2.2 to reverse proxy BI platform web services deployed on the web application server of your choice:

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<listening port> /dswsbobje

   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

   Where `<listening port>` is the listening port of your web application server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.20.2 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.

8.20.2.1 To configure Apache Tomcat

To configure the root path for session cookies to work with ISA 2006 as the reverse proxy server, add the following to the `<Connector>` element in `server.xml`:

```
emptySessionPath="true"
```

1. Stop Tomcat
2. Open the server.xml which is located in:

   `<CATALINA_HOME>\conf`
3. Locate the following section in the server.xml file:

   ```
   <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
   <!-- See proxy documentation for more information about using this -->
   <!--
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxS
   pareThreads="75" enableLookups="false"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyPort="80" disableUploadTimeout="true" />
   -->
   ```
4. Uncomment the Connector element by removing `<!--` and `-->`.
5. To configure the root path for session cookies to work with ISA 2006 as the reverse proxy server, add the following to the `<Connector>` element in `server.xml`:

   ```
   emptySessionPath="true"
   ```
6. Modify the value of `proxyPort` to be the reverse proxy server listen port.
7. Add a new `proxyName` attribute to the Connector's attribute list. The value must be the proxy server name which should be resolvable to the correct IP address by Tomcat.

   For example:

   ```
   <!--Define a Proxied HTTP/1.1 Connector on port 8082
   -->
   <!-- See proxy documentation for more information about using
   this -->
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" emptySessionPath="true"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyName="my_reverse_proxy_server.domain.com"
   proxyPort="ReverseProxyServerPort"
   disableUploadTimeout="true" />
   ```
8. Save and close the `server.xml` file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9. Restart Tomcat.

Ensure the reverse proxy server maps its virtual path to the correct Tomcat connector port. In the above example, the port is 8082.

8.20.2.2 To configure Sun Java 8.2

You need to modify the `sun-web.xml` for every BI platform 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 steps1-4 for every web application.

8.20.2.3 To configure Oracle Application Server 10gR3

You need to modify the `global-web-application.xml` or `orion-web.xml` for every BI platform 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. Log onto the Oracle Admin Console:
   a. Go to *OC4J:home* > *Administration* > *Server Properties*.
   b. Select *Options* under *Command Line Options*.
   c. Click *Add another Row* and type the following:

```
Doracle.useSessionIDFromCookie=true
```

6. Restart the Oracle server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8.20.2.4 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.

8.20.3 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 BI launch pad and BI platform web services have been successfully enabled.

8.20.3.1 To adjust the default viewer URL in the CMC

1. Log on to the CMC.
2. On the *Applications* page, click *Central Management Console*.
3. Select *Actions* > *Processing Settings*.
4. In the *URL* field, select the correct default viewer URL, and click *Save & Close*.
   For example:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   `ReverseProxyServer` and `ReverseProxyServerPort` are the correct reverse proxy server name and its listen port.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9 Authentication

9.1 Authentication options in the BI platform

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

Security plugins expand and customize the ways in which the BI platform authenticates users. Security plugins facilitate account creation and management by allowing you to map user accounts and groups from third-party systems into the platform. You can map third-party user accounts or groups to existing BI platform user accounts or groups, or you can create new Enterprise user accounts or groups that correspond to each mapped entry in the external system.

The current release supports the following authentication methods:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

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

Related Information

Enterprise authentication overview [page 203]
Configuring SAP authentication [page 271]
Using LDAP authentication [page 217]
Windows AD support requirements and initial setup [page 237]
Enabling JD Edwards EnterpriseOne authentication [page 313]
Enabling Oracle EBS authentication [page 322]
Enabling PeopleSoft Enterprise authentication [page 299]
Enabling Siebel authentication [page 318]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.1.1 Primary authentication

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

- If single sign-on is not configured, the user provides their credentials, such as their user name, password and authentication type.
  These details are entered by the users on the logon screen.
- 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 platform server.

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

For instance, if the user is logging on to BI launch pad and specifies Enterprise authentication, the SDK ensures that the BI platform security plug-in performs the authentication. The Central Management Server (CMS) uses the security plug-in to verify the user name and password against the system database. Alternatively, if the user specifies a different authentication method, the SDK uses the corresponding security plug-in to authenticate the user.

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.1.2 Security plug-ins

Security plug-ins expand and customize the ways in which the BI platform authenticates users. The BI platform currently ships with the following plugins:

- Enterprise
- LDAP
- Windows AD
- SAP
- 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 the BI platform. You can map third-party user accounts or groups to existing BI platform user accounts or groups, or you can create new Enterprise user accounts or groups that correspond to each mapped entry in the external system.

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

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

Each security plug-in acts as an authentication provider that verifies user credentials against the appropriate user database. When users log on to the BI platform, they choose from the available authentication types that you have enabled and set up in the Authentication management area of the CMC.

> **Note**
>
> The Windows AD security plugin cannot authenticate users if the BI platform server components are running on UNIX.

9.1.3 Single sign-on to the BI platform

Single sign-on to the BI platform means that once users have logged on to the operating system, they can access applications that support SSO without having to provide their credentials again. When a user logs on, a security context for that user is created. This context can be propagated to the BI platform in order to perform SSO.

The term “anonymous single sign-on” also refers to single sign-on to the BI platform, but it specifically refers to the single sign-on functionality for the Guest user account. When the Guest user account is enabled, which it is by default, anyone can log on to the BI platform as Guest and will have access to the system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.1.3.1 Single sign-on support

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

Single sign-on to BI launch pad can be provided by the BI platform or by different authentication tools, depending on your application server type and operating system.

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

- Windows AD with Kerberos
- Windows AD with SiteMinder

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

- Windows AD with Kerberos
- Windows AD with NTLM
- Windows AD with SiteMinder

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

- LDAP with SiteMinder
- Trusted Authentication
- Windows AD with Kerberos
- LDAP through Kerberos on SUSE 11
- SAP NetWeaver SSO through Trusted Authentication

> **Note**
>
> Windows AD with Kerberos is supported if the Java application is on UNIX. However, BI platform services need to run on a Windows server.

The following table describes the methods of single sign-on support for BI launch pad.

Authentication Mode	CMS Server	Options	Notes
Windows AD	Windows only	Windows AD with Kerberos only	Windows AD authentication to BI launch pad and CMC is available out of the box.
LDAP	Any supported platform	Supported LDAP directory servers, with SiteMinder only	LDAP authentication to the BI launch pad and CMC is available out of the box. SSO to the BI launch pad and CMC requires SiteMinder.
Enterprise	Any supported platform	Trusted Authentication	Enterprise authentication to the BI launch pad and CMC is available out of the box. SSO with enterprise authentication to the BI launch pad and CMC requires Trusted Authentication.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Single sign-on to the BI platform [page 201]
- Single sign-on to the database [page 203]
- End-to-end single sign-on [page 203]

9.1.3.2 Single sign-on to the database

Once users are logged on to the BI platform, single sign-on to the database enables them to perform actions that require database access, in particular, viewing and refreshing reports without having to provide their logon credentials again. Single sign-on to the database can be combined with single sign-on to the BI platform, to provide users with even easier access to the resources they need.

9.1.3.3 End-to-end single sign-on

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

In the BI platform, end-to-end single sign-on is supported through Windows AD and Kerberos.

9.2 Enterprise authentication

9.2.1 Enterprise authentication overview

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

➔ Tip

Use the system default Enterprise authentication if you prefer to create distinct accounts and groups for use with the BI platform, or if you have not already set up a hierarchy of users and groups in a third-party directory server.

You do not have to configure or enable Enterprise authentication. You can however modify Enterprise authentication settings to meet your organization's particular security requirements. You can modify Enterprise authentication settings through the Central Management Console (CMC).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.2.2 Enterprise authentication settings

Settings	Options	Description
Password Restrictions	*Enforce mixed-case password*	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.
User Restrictions	*Must change password every N day(s)*	This option ensures that the passwords do not become a liability and are regularly refreshed.
	Cannot reuse the N most recent passwords(s)	This option ensures that passwords will not routinely be repeated.
	Must wait N minute(s) to change password	This option ensures that new passwords cannot be immediately changed once entered into the system.
Logon Restrictions	*Disable account after N failed attempts to log on*	This security option specifies how many attempts a user is allowed to log on to the system before their account is disabled.
	Reset failed logon count after N minute(s)	This option specifies a time interval for resetting the logon attempt counter.
	Re-enable account after N minute(s)	This option specifies for how long an account is suspended after N failed logon attempts.
Synchronize Data Source Credentials with Log On	*Enable and update user's data source credentials at logon time*	This option enables data source credentials after the user has logged on.
Trusted Authentication	*Trusted Authentication is enabled*	Provides the settings for setting up Trusted Authentication.

Related Information

Enabling Trusted Authentication [page 206]

9.2.3 To change Enterprise settings

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Enterprise*.
   The *Enterprise* dialog box appears.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Change the settings.

> **Tip**
>
> To revert all the settings to the default value click *Reset*.

4. Click *Update* to save your modifications.

9.2.3.1 To change general password settings

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

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

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

   Table 36:

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

4. Click *Update*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Idle Enterprise accounts are not automatically disabled. System administrators have to manually delete accounts that are no longer active.

9.2.4 Enabling Trusted Authentication

Enterprise Trusted Authentication is used to perform single sign-on by relying on the web application server to verify the identity of a user. This method of authentication involves establishing trust between the Central Management Server (CMS) and the web application server hosting the BI platform web application. When the trust is established, the system defers the verification of the identity of a user to the web application server. Trusted Authentication can be used to support authentication methods such as SAML, x.509, and other methods which do not have dedicated authentication plugins.

Users prefer to log on to the system once, without needing to provide passwords several times during a session. Trusted Authentication provides a Java single sign-on solution for integrating your BI platform authentication solution with third-party authentication solutions. Applications that have established trust with the Central Management Server (CMC) can use Trusted Authentication to allow users to log on without providing their passwords.

To enable Trusted Authentication you must configure 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 the BI platform.
> - The single sign-on URL for BI launch pad is `http://server:port/BOE/BI`.

Related Information

To configure the server to use Trusted Authentication [page 206]
To configure Trusted Authentication for the web application [page 210]

9.2.4.1 To configure the server to use Trusted Authentication

Before you can configure Trusted Authentication, you must have created Enterprise users or mapped third-party users who need to sign on to the BI platform.

1. Log on to the CMC.
2. Go to the *Authentication* management area.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Click the *Enterprise* option.
   The *Enterprise* dialog box appears.
4. Under *Trusted Authentication*:
   a. Click *Trusted Authentication is enabled*.
   b. Click *New Shared Secret*.
      The `Shared secret key is generated and ready for download` message appears.
   c. Click *Download Shared Secret*.

      The shared secret is used by the client and the CMS to establish trust. You must first configure the server and then configure the client for Trusted Authentication.

      The *File Download* dialog box appears.
   d. Click *Save*, and save the `TrustedPrincipal.conf` file to one of the following directories:
      - **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
      - **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

      > **Caution**
      >
      > Do not set the timeout to **0** (zero). A **0** value means the amount of time the two clock times can differ is unlimited, which may increase your vulnerability to replay attacks.

   e. In the *Shared Secret Validity Period* field, enter the number of days for the shared secret to be valid.
   f. Specify the maximum amount of time, in milliseconds, that clocks on the client and on the CMS can differ for Trusted Authentication requests.
5. Click *Update* to commit the shared secret.

The BI platform does not audit all modifications to Trusted Authentication parameters. You must manually back up Trusted Authentication information.

The shared secret is used by the client and the CMS to establish trust. The next step is configuring the client for Trusted Authentication.

9.2.5 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`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- 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.

9.2.5.1 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 the BI platform.

Enabling SAML authentication

If your application server can work as a SAML service provider, you can use Trusted Authentication to provide SAML SSO to the BI platform.

To do this, you must first configure the web application server for SAML authentication.

Also, you must use one of these methods to pass the user name to the client:

- REMOTE_USER
- USER_PRINCIPAL

The example below contains a sample web.xml configured for SAML authentication:

```
<security-constraint>
      <web-resource-collection>
        <web-resource-name>InfoView</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>j2ee-admin</role-name>
        <role-name>j2ee-guest</role-name>
        <role-name>j2ee-special</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <login-config>
      <auth-method>FORM</auth-method>
      <realm-name>InfoView</realm-name>
      <form-login-config>
        <form-login-page>/logon.jsp</form-login-page>
        <form-error-page>/logon.jsp</form-error-page>
      </form-login-config>
    </login-config>
    <security-role>
      <description>Assigned to the SAP J2EE Engine System Administrators</
description>
      <role-name>j2ee-admin</role-name>
    </security-role>
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
    <security-role>
      <description>Assigned to all users</description>
      <role-name>j2ee-guest</role-name>
    </security-role>
    <security-role>
      <description>Assigned to a special group of users</description>
      <role-name>j2ee-special</role-name>
    </security-role>
```

Please refer to your application server documentation for further instructions on how to accomplish this, as they will vary by application server.

Using Trusted Authentication

Once your web application server is configured to work as a SAML service provider, you can use Trusted Authentication to provide SAML SSO.

> **Note**
>
> Users must either be imported into the BI platform 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 BI platform account credentials. Once the user's credentials are verified, the system will alias the user's SAML identity to their BI platform account. Subsequent logon attempts for the user will be performed using SSO, as the system will have the user's identity alias dynamically matched to an existing account.

> **Note**
>
> A specific property for the BOE war file - `trusted.auth.user.namespace.enabled` - must be enabled for this mechanism to work.

9.2.5.2 Trusted Authentication properties for web applications

The following table lists Trusted Authentication settings in the default `global.properties` for the `BOE.war` file. To overwrite the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Property	Default value	Description
`sso.enabled=true`	`sso.enabled=false`	Enables and disables single sign-on (SSO) to the BI platform. Set to `true` to enable Trusted authentication.
`trusted.auth.shared.secret`	None	Session variable name used to retrieve the secret for Trusted Authentication.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Default value	Description
		Only applies if using the web session to pass the shared secret.
`trusted.auth.user.param`	None	Specifies the variable used to retrieve the user name for Trusted Authentication.
`trusted.auth.user.retrieval`	None	Specifies the method used to retrieve the user name for Trusted Authentication: • `REMOTE_USER` • `HTTP_HEADER` • `COOKIE` • `QUERY_STRING` • `WEB_SESSION` • `USER_PRINCIPAL` Set to blank to disable Trusted Authentication.
`trusted.auth.user.namespace.enabled`	None	Enables and disables dynamic binding of aliases to existing user accounts. If set to `true`, Trusted Authentication uses alias binding to authenticate users to the BI platform. With alias binding, your application server can work as a SAML service provider, enabling Trusted Authentication to provide SAML single sign-on to the system. If this property is blank, Trusted Authentication will use name matching when authenticating users.

9.2.5.3 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 stored in the appropriate platform directory:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 37:

Platform	Location of TrustedPrincipal.conf
Windows, default installation	• <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ • <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\
AIX	<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/
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 computer hosting the web applications:
   <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.

   Later, you must redeploy the modified BOE.war file.
2. Create a new file, using Notepad or another text editing utility.
3. Enter the following Trusted Authentication properties:

```
sso.enabled=true
trusted.auth.user.retrieval=<Method for user ID retrieval>
trusted.auth.user.param=<Variable>
trusted.auth.shared.secret=<WEB_SESSION>
```

   For the trusted.auth.shared.secret property, select one of the following options for user name retrieval:

   Table 38:

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 trusted.auth.user.param property.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	How the user name will be retrieved
QUERY_STRING	The user name is retrieved from a parameter of the request URL. You specify which query string to use in the trusted.auth.user.param property.
COOKIE	The user name is retrieved from a specified cookie. You specify which cookie to use in the trusted.auth.user.param 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 trusted.auth.user.param property in global.properties.
REMOTE_USER	The user name is retrieved from a call to HttpServletRequest.getRemoteUser().
USER_PRINCIPAL	The user name is retrieved from a call to getUserPrincipal().getName() on the HttpServletRequest object for the current request in a servlet or JSP.

> **Note**
>
> Some web application servers require the environment variable REMOTE_USER set to true on the server. To find out whether this is required, see your web application server documentation. If it is required, confirm that the environment variable is set to true.

> **Note**
>
> If you are using USER_PRINCIPAL or REMOTE_USER to pass the user name, leave the trusted.auth.user.param blank.

4. Save the file with the name global.properties.
5. Restart the web application server.

The new properties take effect only after the modified BOE web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.2.5.3.1 Sample configurations

9.2.5.3.1.1 To pass the shared secret through the TrustedPrincipal.conf file

The following sample configuration assumes that a user called "JohnDoe" has been created in the BI platform.

User information is stored and passed through the web session, and the shared secret is passed via the `TrustedPrincipal.conf` file, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` directory. The bundled version of Tomcat is the web application server.

1. In the **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory, create a new file, using Notepad or any other text editing utility.
2. To specify Trusted Authentication properties, enter the following values:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

3. Save the file with the name **`global.properties`**.
4. Locate the `custom.jsp` file inside the `web` folder in the `com.businessobjects.webpath.InfoView.jar` file at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.
5. Make the following changes to the `custom.jsp` file in the `com.businessobjects.webpath.InfoView.jar` file:

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("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 `web\noCacheCustomResources` folder in the `com.businessobjects.webpath.InfoView.jar` file at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.
7. Add the following values to `myScript.js`:

```
function goToLogonPage() {
    window.location = "logon.jsp"; }
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8. Restart the web application server.
9. Use WDeploy to redeploy the WAR file on the web application server.

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

To verify that you have properly configured Trusted Authentication, use the following URL to access BI launch pad: `http://<[cmsname]>:8080/BOE/BI/custom.jsp` where **<[cmsname]>** is the name of the machine hosting the CMS. The following link should appear: `Click this to go to the logon page of BI launch pad`.

9.2.5.3.1.2 To pass the shared secret through the web session variable

The following sample configuration assumes that a user **<JohnDoe>** has been created in the BI platform.

The user information will be stored and passed via the web session, while the shared secret will be passed via the web session variable. This file is assumed to be in the following directory: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. You need to open and note the content of the file. In this sample configuration, it is assumed the shared secret is the following:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

The bundled version of Tomcat is the web application server.

1. Access the following directory:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Create a new file using a text editor.
3. Specify the trusted authentication properties by entering the following:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```
4. Save the file under the following name:

   global.properties
5. Access the following file:

   `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`
6. Modify the contents of the file to include the following:

   ```
   <\!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","9ecb0778edcff048edae0fcdde1a5db8211
   2934
   86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345
   ```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
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>
```

7. Create the `myScript.js` file in the following directory:

   `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`

8. Add the following to `myScript.js`:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Restart the web application server.
10. Use WDeploy to redeploy the WAR file on the web application server.

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

To verify that you have properly configured Trusted authentication, use the following URL to access the BI launch pad application: `http://[cmsname]:8080/BOE/BI/custom.jsp` where [cmsname] is the name of the machine hosting the CMS. The following link should be displayed:
Click this to go to the logon page of BI launch pad

9.2.5.3.1.3 To pass the user name through user principal

The following sample configuration assumes that a user called “JohnDoe” has been created in the BI platform.

User information is stored and passed through the User Principal option, and the shared secret is passed via the `TrustedPrincipal.conf` file, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` directory. The bundled version of Tomcat is the web application server.

1. Stop the Tomcat server.
2. Open the `server.xml` file for Tomcat, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\` directory.
3. Locate the `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>`, and change it to the following value:

```
Realm className="orgapachecatalinarealmMemoryRealm".../
```

4. Open the `tomcat-users.xml` file, located by default in the `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\` directory.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. Locate the `<tomcat-users>` tag and modify the following value:

```
<user name="JohnDoe" password="password"
roles="onjavauser"/>
```

6. Open the `web.xml` file in the `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` directory.
7. Before the `</web-app>` tag, add the following values:

```
<security-constraint>
    <web-resource-collection>
         <web-resource-name>OnJavaApplication</web-resource-name>
         <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
         <role-name>onjavauser</role-name>
    </auth-constraint>
</security-constraint>

<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>OnJava Application</realm-name>
</login-config>
```

   Enter a specific page for the `<url-pattern></url-pattern>` parameter. Typically, this page is not the default URL for BI launch pad or any other web application.
8. In the custom `global.properties` file, enter the following values:

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

> **Note**
>
> Setting `trusted.auth.user.namespace.enabled=true` is optional. Add the parameter when you want to map an external user name to a different BI platform user name.

9. Restart the web application server.
10. Use WDeploy to redeploy the WAR file on the web application server.

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

The configurations on the web application server are the same if using the Remote User method.

To verify that you have properly configured Trusted authentication, use the following URL to access BI launch pad: `http://<[cmsname]>:8080/BOE/BI`, where **`<[cmsname]>`** is the name of the machine hosting the CMS. After a few moments, a logon dialog box appears.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.3 LDAP authentication

9.3.1 Using LDAP authentication

This section provides a general description of how LDAP authentication works with the BI platform. It then introduces the administration tools that allow you to manage and configure LDAP accounts to the platform.

When you install the BI platform, the LDAP authentication plug-in is installed automatically, but not enabled by default. To use LDAP authentication, you need to first ensure that you have your respective LDAP directory set up. For more information about LDAP, refer to your LDAP documentation.

Lightweight Directory Access Protocol (LDAP), a common, application-independent directory, enables users to share information among various applications. Based on an open standard, LDAP provides a means for accessing and updating information in a directory.

LDAP is based on the X.500 standard, which uses a directory access protocol (DAP) to communicate between a directory client and a directory server. LDAP is an alternative to DAP because it uses fewer resources and simplifies and omits some X.500 operations and features.

The directory structure within LDAP has entries arranged in a specific schema. Each entry is identified by its corresponding distinguished name (DN) or common name (CN). Other common attributes include the organizational unit name (OU), and the organization name (O). For example, a member group may be located in a directory tree as follows: cn=BI platform Users, ou=Enterprise Users A, o=Research. Refer to your LDAP documentation for more information.

Because LDAP is application-independent, any client with the proper privileges can access its directories. LDAP offers you the ability to set up users to log on to the BI platform through LDAP authentication. It provides users with access rights to objects in the system. As long as you have an LDAP server (or servers) running, and use LDAP in your existing networked computer systems, you can use LDAP authentication (along with Enterprise, and Windows AD authentication).

If desired, the LDAP security plug-in provided with the BI platform can communicate with your LDAP server using an SSL connection established using either server authentication or mutual authentication. With server authentication, the LDAP server has a security certificate which the BI platform uses to verify that it trusts the server, while the LDAP server allows connections from anonymous clients. With mutual authentication, both the LDAP server and the BI platform have security certificates, and the LDAP server must also verify the client certificate before a connection can be established.

The LDAP security plug-in provided with the BI platform can be configured to communicate with your LDAP server via SSL, but always performs basic authentication when verifying users' credentials. Before deploying LDAP authentication in conjunction with the BI platform, ensure that you are familiar with the differences between these LDAP types. For details, see RFC2251, which is currently available at http://www.faqs.org/rfcs/rfc2251.html .

Related Information

Configuring LDAP authentication [page 218]
Mapping LDAP groups [page 228]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.3.1.1 LDAP security plugin

The LDAP security plug-in allows you to map user accounts and groups from your LDAP directory server to the BI platform; it also enables the system to verify all logon requests that specify LDAP authentication. Users are authenticated against the LDAP directory server, and have their membership in a mapped LDAP group verified before the CMS grants them an active BI platform session. User lists and group memberships are dynamically maintained by the system. You can specify that the platform use a Secure Sockets Layer (SSL) connection to communicate to the LDAP directory server for additional security.

LDAP authentication for the BI platform is similar Windows AD authentication in that you can map groups and set up authentication, access rights, and alias creation. Also as with NT or AD authentication, you can create new Enterprise accounts for existing LDAP users, and can assign LDAP aliases to existing users if the user names match the Enterprise user names. In addition, you can do the following:

- Map users and groups from the LDAP directory service.
- Map LDAP against AD. There are a number of restrictions if you configure LDAP against AD.
- Specify multiple host names and their ports.
- Configure LDAP with SiteMinder.

Once you have mapped your LDAP users and groups, all of the BI platform client tools support LDAP authentication. You can also create your own applications that support LDAP authentication.

Related Information

Configuring SSL settings for LDAP Server or Mutual Authentication [page 222]
Mapping LDAP against Windows AD [page 229]
Configuring the LDAP plug-in for SiteMinder [page 226]

9.3.2 Configuring LDAP authentication

To simplify administration, the BI platform supports LDAP authentication for user and group accounts. Before users can use their LDAP user name and password to log on to the system, you need to map their LDAP account to the BI platform. When you map an LDAP account, you can choose to create a new account or link to an existing BI platform account.

Before setting up and enabling LDAP authentication, ensure that you have your LDAP directory set up. For more information, refer to your LDAP documentation.

Configuring LDAP authentication includes the following tasks:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.

9.3.2.1 To configure the LDAP host

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

1. Select *Authentication* from the navigation list to go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.
3. If you are setting up LDAP authentication for the first time, click *Start LDAP Configuration Wizard*.
4. Enter the name and port number of your LDAP hosts in the *Add LDAP host (hostname:port)* field (for example, "myserver:123"), click *Add*, and then click *Next*.

   > **Tip**
   >
   > Repeat this step to add more than one LDAP host of the same server type if you want to add hosts that can act as failover servers. If you want to remove a host, highlight the host name and click *Delete*.

5. Select your server type from the *LDAP Server Type* list.

   > **Note**
   >
   > If you are mapping LDAP to AD, select *Microsoft Active Directory Application Server* for your server type.

6. If you want to view or change any of the LDAP server attribute mappings or LDAP default search attributes, click *Show Attribute Mappings*.

   By default, each supported server type's server attribute mappings and search attributes are set.
7. Click *Next*.
8. In the *Base LDAP Distinguished Name* field, type the distinguished name (for example, o=SomeBase) for your LDAP server, and click *Next*.
9. In the *LDAP Server Administration Credentials* area, specify the distinguished name and password for a user account that has read access to the directory.

   Administrator credentials are not required.

   If your LDAP Server allows anonymous binding, leave this area blank. BI platform servers and clients will bind to the primary host via anonymous logon.
10. If you have configured referrals on your LDAP host, enter the authentication information in the *LDAP Referral Credentials* area and enter the number of referral hops in the *Maximum Referral Hops* field.

    You must configure the *LDAP Referral Credentials* area if all of the following criteria apply:

    - The primary host has been configured to refer to another directory server that handles queries for entries under a specified base.
    - The host being referred to has been configured to not allow anonymous binding.
    - A group from the host being referred to will be mapped to the BI platform.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Although groups can be mapped from multiple hosts, only one set of referral credentials can be set. Therefore, if you have multiple referral hosts, you must create a user account on each host that uses the same distinguished name and password.

> **Note**
>
> If *Maximum Referral Hops* is set to zero, no referrals will be followed.

11. Click *Next*.
12. Choose the type of Secure Sockets Layer (SSL) authentication used:
    - *Basic (no SSL)*
    - *Server Authentication*
    - *Mutual Authentication*

    Details and prerequisites for both Server and Mutual authentication are discussed in a subsequent section. To successfully set up LDAP authentication using either type of SSL, review *Configuring SSL settings for LDAP Server or Mutual Authentication* in this document before proceeding further in this procedure.
13. Click *Next*, and select a method of LDAP single sign-on authentication:
    - *Basic (no SSO)*
    - *SiteMinder*
14. Click *Next*, and select how aliases and users are mapped to BI platform accounts.
    a. In the *New Alias Options* area, select how new aliases are mapped to Enterprise accounts:
       - *Assign each added LDAP alias to an account with the same name*
         Use this option when you know users have an Enterprise account with the same name; that is, LDAP aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and LDAP account, are added as new users.
       - *Create a new account for every added LDAP alias*
         Use this option when you want to create a new account for each user.

    b. In the *Alias Update Options* area, select how to manage alias updates for the Enterprise accounts:
       - *Create new aliases when the Alias Update occurs*
         Use this option to automatically create a new alias for every LDAP user mapped to the BI platform. New LDAP accounts are added for users without BI platform accounts or for all users if you selected *Create a new account for every added LDAP alias*.
       - *Create new aliases only when the user logs on*
         Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use the BI platform. The system does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.

    c. In the *New User Options* area, specify how new users are created:
       - *New users are created as named users*
         New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

connected. You must have a named user license available for each user account created using this option.

- *New users are created as concurrent users*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the platform, a 100-user concurrent license could support 250, 500, or 700 users.

15. Perform this step if you are setting up user attribute mappings or if you plan to import email addresses from the LDAP server. In the *Attribute Binding Options* area, specify the attribute binding priority for the LDAP plugin:
    a. Click the *Import Full Name, Email Address and other attributes* box.
    The full names and descriptions used in the LDAP accounts are imported and stored with the user objects in the system.
    b. Specify an option for *Set priority of LDAP attribute binding relative to other attribute bindings*.

> **Note**
>
> If the option is set to 1, LDAP attributes take priority in scenarios where LDAP and other plugins (Windows AD and SAP) are enabled. If the option is set to 3, attributes from other enabled plugins will take priority.

16. Click *Finish* .

Related Information

Configuring SSL settings for LDAP Server or Mutual Authentication [page 222]
Configuring the LDAP plug-in for SiteMinder [page 226]

9.3.2.2 Managing multiple LDAP hosts

When using LDAP and the BI platform, you can add fault tolerance to your system by adding multiple LDAP hosts. The system uses the first host that you add as the primary LDAP host. Subsequent hosts are treated as failover hosts.

The primary LDAP host and all failover hosts must be configured in exactly the same way, and each LDAP host must refer to all additional hosts from which you want to map groups. For more information about LDAP hosts and referrals, see your LDAP documentation.

To add multiple LDAP Hosts, enter all hosts when you configure LDAP using the LDAP configuration wizard (see for details.) Or if you have already configured LDAP, go to the Authentication management area of the Central Management Console and click the LDAP tab. In the LDAP Server Configuration Summary area, click the name of the LDAP host to open the page that enables you to add or delete hosts.

> **Note**
>
> Make sure that you add the primary host first, followed by the remaining failover hosts.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> If you use failover LDAP hosts, you cannot use the highest level of SSL security (that is, you cannot select "Accept server certificate if it comes from a trusted Certificate Authority and the CN attribute of the certificate matches the DNS hostname of the server.")

Related Information

Configuring LDAP authentication [page 218]

9.3.2.3 Configuring SSL settings for LDAP Server or Mutual Authentication

This section contains detailed information on Server or Mutual SSL-based authentication for LDAP. Preliminary steps are required for setting up SSL-based authentication. This section also provides specific information for configuring SSL with LDAP Server and Mutual Authentication in the CMC. It assumes that you have configured the LDAP host and that you selected either of these for your SSL authentication choice:

For additional information or for information on configuring the LDAP host server, refer to your LDAP vendor documentation.

Related Information

To configure the LDAP host [page 219]

9.3.2.3.1 To configure the LDAP Server or Mutual Authentication

Resource	Take this action before starting this task
CA certificate	This action is required for both server and Mutual Authentication with SSL. 1. Obtain a Certificate Authority (CA) to generate a CA certificate. 2. Add the certificate to your LDAP Server. For information, see your LDAP vendor documentation.
Server certificate	This action is required for both server and Mutual Authentication with SSL.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Resource	Take this action before starting this task
	1. Request and then generate a server certificate. 2. Authorize the certificate and then add it to the LDAP Server.

cert7.db or cert8.db, key3.db	These files are required for both server and Mutual Authentication with SSL.
	1. Download the certutil application that generates either a `cert7.db` or `cert8.db` file (depending on your requirements) from https://developer.mozilla.org/en-US/docs/NSS/tools .
	2. Copy the CA certificate to the same directory as the certutil application.
	3. Use the following command to generate the `cert7.db` or `cert8.db`, `key3.db`, and `secmod.db` files:
	`certutil -N -d .`
	4. Use the following command to add the CA certificate to the `cert7.db` or `cert8.db` file:
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	5. Store the three files in a directory on the computer that hosts the BI platform.

cacerts	This file is required for server or Mutual Authentication with SSL for Java applications, like BI launch pad. 1. Locate the `keytool` file in your Java `bin` directory. 2. Use the following command to create the `cacerts` file: `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` 3. Store the `cacerts` file in the same directory as the `cert7.db` or `cert8.db` and `key3.db` files.
Client certificate	1. Create separate client requests for the `cert7.db` or `cert8.db` and `.keystore` files: ○ To configure the LDAP plugin, use the certutil application to generate a client certificate request. ○ Use the following command to generate the client certificate request: `certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .` `<client_dn>` includes information such as "CN=**<client_name>**, OU=**<org unit>**, O=**<Companyname>**, L=**<city>**, ST=**<province>**, and C=**<country>**.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Resource	Take this action before starting this task

	2. Use the CA to authenticate the certificate request. Use the following command to retrieve the certificate and insert it in the `cert7.db` or `cert8.db` file:
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. To facilitate Java authentication with SSL:
	○ Use the keytool utility in the Java `bin` directory to generate a client certificate request.
	○ Use the following command to generate a key pair:
	`keytool -genkey -keystore .keystore`
	4. After specifying information about your client, use the following command to generate a client certificate request:
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. After the client certificate request is authenticated by the CA, use the following command to add the CA certificate to the `.keystore` file:
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. Retrieve the client certificate request from the CA, and use the following command to add it to the `.keystore` file:
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. Store the `.keystore` file in the same directory as the `cert7.db` or `cert8.db` and `cacerts` files on the computer that hosts the BI platform.

1. Choose the level of SSL security to use.

   If you are using the LDAP configuration wizard to configure LDAP authentication for the first time, select *Mutual Authentication* from the *Type of SSL authentication* list, and click *Next*. Or, if you are reconfiguring your LDAP authentication configuration, go to the *Authentication* area of the CMC, and double-click *LDAP*. The *LDAP Server Configuration Summary* page appears. Click the *SSL Type* value, and select *Mutual Authentication* from the *Type of SSL authentication* list.

   - *Always accept server certificate*
     This is the lowest security option. Before BI platform can establish an SSL connection with the LDAP host (to authenticate LDAP users and groups), it must receive a security certificate from the LDAP host. The BI platform does not verify the certificate it receives.
   - *Accept server certificate if it comes from a trusted Certificate Authority*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This is a medium security option. Before the BI platform can establish an SSL connection with the LDAP host (to authenticate LDAP users and groups), it must receive and verify a security certificate sent to it by the LDAP host. To verify the certificate, the system must find the CA that issued the certificate in its certificate database.

- *Accept server certificate if it comes from a trusted Certificate Authority, and the CN attribute of the certificate matches the DNS hostname of the server*
  This is the highest security option. Before the BI platform can establish an SSL connection with the LDAP host (to authenticate LDAP users and groups), it must receive and verify a security certificate sent to it by the LDAP host. To verify the certificate, the BI platform must find the CA that issued the certificate in its certificate database and be able to confirm that the CN attribute on the server certificate exactly matches the LDAP host name you entered in the *Add LDAP host* box in the first step of the wizard—if you entered the LDAP host name as `ABALONE.rd.crystald.net:389`. (Using `CN =ABALONE:389` in the certificate doesn't work.) .
  The host name on the server security certificate is the name of the primary LDAP host. If you select this option, you cannot use a failover LDAP host.

> **Note**
>
> Java applications ignore the first and last setting and accept the server certificate only if it comes from a trusted CA.

2. In the *SSL host* box, type the host name of each computer, and click *Add*.

   Next, you must add the host name of each computer in your BI platform deployment that uses the BI platform SDK. (This includes the computer running your Central Management Server and the computer running your web application server.)
3. Specify the SSL settings for each SSL host you added to the list:
   a. Select *default* in the SSL list.
   b. Clear the *Use default value* check boxes.
   c. Type a value in the *Path to the certificate and key database files* box and the *Password for the key database* box.
   d. If specifying settings for mutual authentication, type a value in the *Nickname for the client certificate in the certificates database* box.

> **Note**
>
> The default settings will be used (for any setting) for any host with the *Use default value* check box selected or for any computer name you do not add to the list of SSL hosts.

4. Specify the default settings for each host that isn't in the list, and click *Next*.

   To specify settings for another host, select the host name in the list on the left, and type values in the boxes on the right.

> **Note**
>
> The default settings will be used for any setting (for any host) with the *Use default value* check box selected or for any computer name you do not add to the list of SSL hosts.

5. Select *Basic (no SSO)* or *SiteMinder* as the method of LDAP single sign-on authentication.
6. Choose how new LDAP users and aliases are created.
7. Click *Finish*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Configuring the LDAP plug-in for SiteMinder [page 226]

9.3.2.4 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 on the *LDAP Server Configuration Summary* page.

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   If LDAP authentication is configured, the *LDAP Server Configuration Summary* page appears. On this page, you can change any connection parameter areas or fields and modify options in the *Mapped LDAP Member Groups* area.
3. Delete currently mapped groups that will no longer be accessible under the new connection settings, and click *Update*.

   You can delete mapped groups by selecting the user group and then clicking the *Delete* button in the *Mapped LDAP Member Groups* section.
4. Change your connection settings, and click *Update*.
5. Change your *New Alias Options*, *Alias Update Options*, and *New User Options* if necessary, and click *Update*.
6. Map your new LDAP member groups, and click *Update*.

9.3.2.5 Configuring the LDAP plug-in for SiteMinder

This section explains how to configure the CMC to use LDAP with SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the LDAP security plug-in to create single sign-on to the BI platform.

To use SiteMinder and LDAP with the BI platform, you need to make configuration changes in two places:

- LDAP plug-in through the CMC
- `BOE.war` file properties

> **Note**
>
> Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done, regardless of what supported version of SiteMinder you are using. For more information about SiteMinder and how to install it, refer to the SiteMinder documentation.

Related Information

To configure the LDAP host [page 219]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.3.2.5.1 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 *Single Sign-On Type* on the LDAP authentication screen, which is available if you have already configured LDAP and are now adding SSO.
2. In the *Policy Server Host* box, type the name of each policy server, and then click *Add*.
3. For each Policy Server Host, specify the *Accounting*, *Authentication* and *Authorization* port numbers.
4. Enter the name of the *Agent Name* and the *Shared Secret*. Re-enter the shared secret in the *Confirm Shared Secret* box.
5. Click *Next*.
6. Proceed with configuring the LDAP options.

9.3.2.5.2 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 **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` directory in your BI platform installation.
2. Create a new file, using Notepad or any other text editing utility.
3. Enter the following statement:

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. Close the file and save it under the **global.properties** name, without a file extension.
5. Create another file in the same directory.
6. Enter the following statement:

```
authentication.default=secLDAP
cms.default=[<your cms name>]:[<the CMS port number>]
```

   For example:

```
authentication.default=secLDAP
cms.default=mycms:6400
```

7. Close the file and save it under the `bilaunchpad.properties` name.

The new properties take effect only after the modified BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.3.3 Mapping LDAP groups

Once you have configured the LDAP host using the LDAP configuration wizard, you can map LDAP groups to Enterprise groups.

Once you have mapped LDAP groups, you can view the groups by clicking the LDAP option in the *Authentication* management area. If LDAP authentication is configured, the Mapped LDAP Member Groups area displays the LDAP groups that have been mapped to the BI platform.

> **Note**
>
> You can also map Windows AD groups to authenticate in the BI platform via the LDAP security plugin.

> **Note**
>
> If you have configured LDAP against AD, this procedure will map your AD groups.

Related Information

Mapping LDAP against Windows AD [page 229]

9.3.3.1 To map LDAP groups using the BI platform

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   If LDAP authentication is configured, the LDAP summary page appears.
3. In the *Mapped LDAP Member Groups* area, specify your LDAP group (either by common name or distinguished name) in the *Add LDAP group (by cn or dn)* field, and click *Add*.

   To add more than one LDAP group, repeat this step. To remove a group, highlight the LDAP group and click *Delete*.
4. In the *New Alias Options* area, select an option to specify how to map LDAP aliases to Enterprise accounts:
   - *Assign each added LDAP alias to an account with the same name*
     Use this option when you know users have an existing Enterprise account with the same name (that is, LDAP aliases will be assigned to existing users—auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and LDAP account, are added as new LDAP users.
   - *Create a new account for every added LDAP alias*
     Use this option when you want to create a new account for each user.
5. In the *Alias Update Options* area, select an option to specify whether LDAP aliases are automatically created for all new users:
   - *Create new aliases when the Alias Update occurs*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Use this option to automatically create a new alias for every LDAP user mapped to the BI platform. New LDAP accounts are added for users without BI platform accounts or for all users if you selected *Create a new account for every added LDAP alias* and clicked *Update*.

- *Create new aliases only when the user logs on*
  Use this option when the LDAP directory you are mapping contains many users, but only a few of them will use the BI platform. The system does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.

6. In the *New User Options* area, if your BI platform license is based on users roles, select an option to specify properties of the new Enterprise accounts that are created to map to LDAP accounts:
   - *New users are created as named users*
     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system, regardless of how many other people are connected. You must have a named user license available for each user account created using this option.
   - *New users are created as concurrent users*
     New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.
7. Click *Update*.

9.3.3.2 To unmap LDAP groups using the BI platform

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   If LDAP authentication is configured, the LDAP summary page will appear.
3. In the "Mapped LDAP Member Groups" area, select the LDAP group you would like to remove.
4. Click *Delete*, and then click *Update*.

   The users in this group will not be able to access the BI platform.

> **Note**
>
> The only exceptions to this occur when a user has an alias to an Enterprise account. To restrict access, disable or delete the user's Enterprise account.

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

9.3.3.3 Mapping LDAP against Windows AD

If you configure LDAP against Windows AD (AD), note the following restrictions:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- If you configure LDAP against AD, you will be able to map your users but you will not be able to configure AD single sign-on or single sign-on to the database. However, LDAP single sign-on methods like SiteMinder and trusted authentication will still be available.
- Users who are only members of default groups from AD will not be able to log in successfully. Users must also be a member of another explicitly created group in AD and, in addition, this group must be mapped. An example of such a group is the "domain users" group.
- If a mapped domain local group contains a user from a different domain in the forest, the user from a different domain in the forest will not be able to log in successfully.
- Users from a universal group from a domain different than the DC specified as the LDAP host will not be able to log in successfully.
- You cannot use the LDAP plug-in to map users and groups from AD forests outside the forest where the BI platform is installed.
- You cannot map in the Domain Users group in AD.
- You cannot map a machine local group.
- If you are using the Global Catalog Domain Controller, there are additional considerations when mapping LDAP against AD:

  Table 39:

Situation	Considerations
Multiple domains when pointing to the Global Catalog Domain Controller	You can map in: ○ universal groups on a child domain, ○ groups on the same domain that contains universal groups from a child domain, and ○ universal groups on a cross domain. You cannot map in: ○ global groups on a child domain, ○ local groups on a child domain, ○ groups on the same domain that contain a global group from the child domain, and ○ cross-domain global groups. Generally, if the group is a universal group, it will support users from cross or child domains. Other groups will not be mapped if they contain users from cross or child domains. Within the domain you are pointing to, you can map domain local, global, and universal groups.
Mapping in universal groups	To map in universal groups, you must point to the Global Catalog Domain Controller. You should also use port number 3268 instead of the default 389.

- If you are using multiple domains but not pointing to the Global Catalog Domain Controller, then you cannot map in any type of groups from cross or child domains. You can map in all types of groups only from the specific domain you are pointing to.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.3.3.4 Using the LDAP plugin to configure SSO to the SAP HANA database

This section provides administrators with the steps required to set up and configure single sign-on (SSO) between the BI platform running on SUSE Linux 11 and the SAP HANA database. LDAP authentication using Kerberos enables AD users to be authenticated on a BI platform running on Linux - specifically SUSE. This scenario also supports single sign-on to SAP HANA as the reporting database.

> **Note**
>
> For information on how to set up the SAP HANA database, see the *SAP HANA Database - Server Installation and Update Guide*. For information on how to set up the Data Access component for SAP HANA, see the *Data Access Guide*.

Implementation overview

The following components must be in place for Kerberos SSO to work.

Table 40:

Component	Requirement
Domain controller	Hosted on a machine running Active Directory setup to use Kerberos authentication.
Central Management Server	Installed and running on a machine running SUSE Linux Enterprise 11 (SUSE).
Kerberos V5 client	Installed together with the required utilities and libraries on the SUSE host. **Note** Use the latest version of the Kerberos V5 client. Add the `bin` and `lib` folders to the `PATH` and `LD_LIBRARY_PATH` environment variables.
LDAP authentication plug-in	Enabled on the SUSE host.
Kerberos login configuration file	Created on the machine hosting the web application server.

Implementation workflow

The following tasks must be performed to enable BI platform users to SSO to SAP HANA using Kerberos authentication through JDBC.

1. Setting up the AD host.
2. Creating accounts and keytab files for the SUSE host and the BI platform on the AD Host.
3. Installing Kerberos resources on the SUSE host.
4. Configuring the SUSE host for Kerberos authentication.
5. Configuring Kerberos authentication options in the LDAP authentication plug-in.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Creating a Kerberos login configuration file for the web application host.

9.3.3.4.1 To set up the domain controller

You may need to set up a trust relationship between the SUSE host and the domain controller. If the SUSE host is in the Windows domain controller, you do not have to set up the trust relationship. However, if the BI platform deployment and the domain controller are in different domains, you may need to set up a trust relationship between the SUSE Linux machine and the domain controller. This would require the following:

1. Create a user account for the SUSE machine running the BI platform.
2. Create a host Service Principal Name (SPN).

> **Note**
>
> The SPN should be formatted according to Windows AD conventions: host/**<hostname>**@**<DNS_REALM_NAME>**. Use, in lowercase, a fully qualified domain name for /**<hostname>**. The **<DNS_REALM_NAME>** should be specified in uppercase.

3. Run the Kerberos keytab setup command `ktpass` to associate the SPN with the user account:

```
c:\> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
```

The following steps must be performed on the machine hosting the domain controller.

1. Create a user account for the service running the BI platform.
2. On the *User Accounts* page, right-click the new service account and select *Properties* > *Delegation*.
3. Select *Trust this user for delegation to any service (Kerberos only)*.
4. Run the Kerberos keytab setup command `ktpass` to create an SPN account for the new service account:

```
c:\>ktpass -princ <sianame>/<service_name>@<DNS_REALM_NAME> -mapuser
<service_name> -pass <password> -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT -
out <sianame>.keytab
```

> **Note**
>
> The SPN should be formatted according to Windows AD conventions: sianame/**<service_name>**@**<DNS_REALM_NAME>**. Specify the **<service name>** in lowercase otherwise your SUSE platform may not be able to resolve it. The **<DNS_REALM_NAME>** should be specified in uppercase.

Table 41:

Parameter	Description
-princ	Specifies the principal name for Kerberos authentication.
-out	Specifies the name of the Kerberos `keytab` file to generate. This should match the **<sianame>** used in -princ.
-mapuser	Specifies the name of the user account to which the is SPN mapped to. The Server Intelligence Agent runs on this account.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description
-pass	Specifies the password used by the service account.
-ptype	Specifies the principal type: `-ptype KRB5_NT_PRINCIPAL`
-crypto	Specifies the encryption type to use with the service account: `-crypto RC4-HMAC-NT`

You have generated the required keytab files for the trust relationship between the SUSE machine and the domain controller.

You must transfer the keytab file(s) to the SUSE machine and store them in the `/etc` directory.

9.3.3.4.2 To set up the SUSE Linux Enterprise 11 machine

The following resources are required for setting up Kerberos on the SUSE Linux machine running the BI platform:

- Keytab files created on the domain controller. The keytab file created for the BI platform service is mandatory. The keytab for the SUSE host is recommended specifically for scenarios where the BI platform host and the domain controller are in different domains.
- The latest Kerberos V5 library (including the Kerberos client) must be installed on the SUSE host. You must add the location of the binaries to the `PATH` and `LD_LIBRARY_PATH` environment variables. To verify that the Kerberos client is properly installed and configured, ensure that the following utilities and libraries exist on the SUSE host:
  - `kinit`
  - `ktutil`
  - `kdestroy`
  - `klist`
  - `/lib64/libgssapi_krb5.so.2.2`
  - `/lib64/libkrb5.so.3.3`
  - `/lib/libkrb5support.so.0.1`
  - `/lib64/libk5crypto.so.3`
  - `/lib64/libcom_err.so.2`

> **Tip**
>
> Run `rpm -qa | grep krb` to check the version of these libraries. For information on the latest Kerberos client, libraries, and Unix host configuration see http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5 .

After all the required resources are available on the SUSE host, follow the instructions below to set up Kerberos authentication.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Note

To perform these steps you must have root privileges.

1. To merge the keytab files, run the following command:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Edit the `/etc/kerb5.conf` file to refer to the domain controller (on the Windows platform) as the Kerberos Domain Controller (KDC).

   Use to the example below:

```
[domain_realm]
 .name.mycompany.corp = DOMAINNAME.COM
  name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
        forwardable = true
           default_realm = DOMAINNAME.COM
           default_tkt_enctypes = rc4-hmac
           default_tgs_enctypes = rc4-hmac

[realms]
        DOMAINNAME.COM = {
             kdc = machinename.domainname.com
            }
```

   ### Note

   The `krb5.conf` file contains Kerberos configuration information, including the locations of KDCs and servers for the Kerberos realms of interest, Kerberos applications, and mappings of hostnames onto Kerberos realms. Normally the `krb5.conf` file is installed in the `/etc` directory.

3. Add the domain controller to `/etc/hosts` so that the SUSE host can locate the KDC.
4. Run the `kinit` program from the `/usr/local/bin` directory to verify that Kerberos has been set up properly. Verify that an AD account user account can log into the SUSE machine.

   ### Tip

   The KDC should issue a Ticket Granting Ticket (TGT) which can be viewed in the cache. Use the `klist` program to view the TGT.

Example

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>

> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

You should also use `kinit` to test the SPNs.

9.3.3.4.3 To configure Kerberos authentication options for LDAP

Before configuring Kerberos authentication for LDAP, you must first enable and configure the BI platform LDAP authentication plugin to connect to the AD directory. To use LDAP authentication, you need to first ensure that you have set up your respective LDAP directory.

> **Note**
>
> When running the *LDAP Configuration Wizard* you must specify *Microsoft Active Directory Application Server* and provide the requested configuration details.

After LDAP authentication is enabled and connected to your Microsoft Active Directory Application Server, the *Enable Kerberos Authentication* area appears on the LDAP Server Configuration Summary page. Use this area to configure Kerberos authentication, which is required for single sign-on to the SAP HANA database from a BI platform deployment on SUSE.

1. Go to the *Authentication* management area of the CMC.
2. Double-click *LDAP*.

   The *LDAP Server Configuration Summary* page appears, where you can modify any of the connection parameters or fields.
3. To configure Kerberos authentication, perform the following steps in the *Enable Kerberos Authentication* area:
   a. Click *Enable Kerberos Authentication*.
   b. Click *Cache Security Context (required for SSO to database)*.

      > **Note**
      >
      > Enabling the cache security context is specifically required for single sign-on to SAP HANA.

   c. Specify the Service Principal Name (SPN) for the BI platform account in *Service Principal Name*.

      The format for specifying the SPN is **<sianame/service>**@**<DNS_REALM_NAME>** where

      Table 42:

<sianame>	Name of the Server Intelligence Agent
<service>	Name of the service account used to run the BI platform
DNS_REALM_NAME	The domain name of the domain controller in uppercase

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Tip**
>
> When specifying the SPN, remember that **<sianame/service>** is case sensitive.

d. Specify the domain for the domain controller in *Default Kerberos Realm*.
e. Specify `userPrincipalName` in *User Principal Name*.

   This value is used by the LDAP authentication application to provide user ID values that are required by Kerberos. The value specified should match the name provided when creating the keytab files.

4. Click *Update* to submit and save your changes.

You have configured Kerberos authentication options to refer to user accounts in the AD directory.

You need to create a Kerberos login configuration file - `bscLogin.conf` - to enable Kerberos logon and single sign-on.

Related Information

Configuring LDAP authentication [page 218]

9.3.3.4.4 To create a Kerberos login configuration file

To enable Kerberos logon and single sign-on, you need to add a login configuration file on the machine hosting the BI platform web application server.

1. Create a file called `bscLogin.conf` and store it in the `/etc` directory.

> **Note**
>
> You can store this file in a different location. However, if you do, you will need to specify its location in your Java options. It is recommended that the `bscLogin.conf` and the Kerberos keytab files reside under the same directory. In a distributed deployment, you must add a `bscLogin.conf` file for every machine hosting a web application server.

2. Add the following code to your login `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="<principal name>";
};
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The following section is specifically required for single sign-on:
>
> ```
> com.businessobjects.security.jgss.accept {
> com.sun.security.auth.module.Krb5LoginModule required
> storeKey=true
> useKeyTab=true
> keyTab="/etc/krb5.keytab"
> principal="<principal name>";
> };
> ```

3. Save and close the file.

9.3.3.5 Troubleshooting new LDAP accounts

- If you create a new LDAP user account, and the account does not belong to a group account that is mapped to the BI platform, either map the group, or add the new LDAP user account to a group that is already mapped to the system.
- If you create a new LDAP user account, and the account belongs to a group account that is mapped to the BI platform, refresh the user list.

Related Information

Configuring LDAP authentication [page 218]
Mapping LDAP groups [page 228]

9.4 Windows AD authentication

9.4.1 Using Windows AD authentication

9.4.1.1 Windows AD support requirements and initial setup

This section guides you through the process of configuring Windows Active Directory (AD) authentication to work on the BI platform. All the required end-to-end workflows you need to perform are presented together with validation tests and prerequisite checks.

Support requirements

To facilitate AD authentication on the BI platform, you should remember the following support requirements.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- The CMS must always be installed on a supported Windows platform.
- Although Windows 2008 is a supported platform for both Kerberos and NTLM authentication, certain BI platform applications may only use particular authentication methods. For example, applications such as BI launch pad and Central Management Console only support Kerberos.

Recommended AD set up workflow

To initially set up manual AD authentication with the BI platform, use the following workflow:

1. Set up the Domain Controller.
2. Configure AD authentication in the CMC.
3. Configure the AD user account on the Server Intelligence Agent (SIA).
4. Configure your web application server for AD authentication with Kerberos.

> **Note**
>
> Use this workflow whether or not you require single sign-on (SSO). The workflow described in the following sections will first enable you to manually (using an AD username and password) log into the BI platform. Once you have successfully configured manual AD authentication, a detailed section is provided to guide you through the process of setting up SSO for AD authentication.

9.4.2 Preparing the Domain Controller

9.4.2.1 Setting up a service account for AD authentication with Kerberos

To configure the BI platform to work with Windows AD (Kerberos) authentication, you require a service account. You can either create a new domain account or use an existing domain account. The service account will be used to run the BI platform servers. After setting up the account, you will need to set up an SPN for the account. This SPN is used to import AD user groups into the BI platform.

> **Note**
>
> To use AD with SSO, you will need to later revisit the service account set up to grant the account appropriate rights, and configure it for constrained delegation.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.2.1.1 To set up the service account on a Windows 2008 domain

You need to set up a new service account to successfully enable Windows AD authentication using the Kerberos protocol. This service account will be used primarily to allow users in a given AD group to log on to BI launch pad. The following task is performed on the AD domain controller machine.

1. Create a new service account with a password on the primary domain controller.
2. Use the `setspn -a` command to add the service principal names (SPN) to the service account you created in Step 1. Specify service principal names (SPNs) for the service account, as well as the server, fully qualified domain server and IP address for the machine on which BI launch pad is deployed.
   For example:

   ```
   setspn -a BICMS/service_account_name.domain.com serviceaccountname
   setspn -a HTTP/<servername> <servicename>
   setspn -a HTTP/<servername.domain.com> <servicename>
   setspn -a HTTP/<ip address of server> <servicename>
   ```

   `BICMS` is the name of the machine on which the SIA is running, **<servername>** is the name of the server on which BI launch pad is deployed and **<servernamedomain>** is its fully qualified domain name.
3. Run `setspn -l` **<servicename>** to verify that the service principal names were added to the service account.
   The output for the command should include all the registered SPNs as shown below:

   ```
   Registered ServicePrincipalNames for
   CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
   HTTP/<ip address of server>
   HTTP/<servername>.DOMAIN.com
   HTTP/<servername>
   <servername>/<servicename>DOMAIN.com
   ```

   A sample output is provided below:

   ```
   C:\Users\Admin>setspn -L bossosvcacct

   Registered ServicePrincipalNames for
   CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
           BICMS/bossosvcacct.domain.com
           HTTP/Tomcat HTTP/Tomcat.domain.com
           HTTP/Load_Balancer.domain.com
   ```

Once created, the service account needs to be granted rights and added to the server's Local Administrators group. The SPN will be used to import AD groups in the next section.

9.4.3 Configuring AD Authentication in the CMC

9.4.3.1 Windows AD security plug-in

The Windows AD security plug-in enables you to map user accounts and groups from your AD 2008 user database to the BI platform. It also enables the system to verify all logon requests that specify AD Authentication. Users are authenticated against the AD user database, and have their membership in a mapped AD group verified

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

before the Central Management Server (CMS) grants them an active session. You can use the plug-in to configure updates for the imported AD groups.

The Windows AD security plug-in enables you to configure the following:

- Windows AD authentication with Kerberos
- Windows AD authentication with NTLM
- Windows AD authentication with SiteMinder for single sign-on

The AD security plug-in is compatible with AD 2008 domains running in either native mode or mixed mode.

Once you have mapped your AD users and groups, they will be able to access BI platform client tools using the *Windows AD* authentication option.

- Windows AD authentication only works if the CMS is run on Windows. For SSO to a database to work, the reporting servers must also run on Windows. Otherwise all other servers and services can run on all platforms supported by the BI platform.
- The Windows AD plug-in for the BI platform supports domains within multiple forests.

9.4.3.2 To map Windows AD users and groups

Before you can import AD user groups into the BI platform, you must have completed the following prerequisite actions:

- Created a service account on the domain controller for the BI platform. The account will be used to run BI platform servers.

  > **Note**
  >
  > To enable AD authentication with Vintela single sign-on (SSO), you must provide an SPN that is configured for this purpose. The steps provided below are for configuring manual AD authentication to the BI platform. Once you have configured manual AD authentication, refer to the *Single Sign-On Setup* section in this chapter for details on how to add SSO to your AD authentication configuration.

- Verified that the SPN containing the name of the machine on which the SIA is running has been added to the service account.

Steps 1 to 11 below are mandatory to import AD groups into the BI platform.

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

   > **Note**
   >
   > Before the Windows AD plug-in is configured, this link appears as quotation marks. After the configuration is saved, the link is populated with AD Administration names.

5. Enter the name and password of an enabled domain user account.

   Administration credentials can use either of the following formats:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

The BI platform uses this account to query information from AD. The platform does not modify, add, or delete content from AD. Because only reads information, only the appropriate rights are required.

> **Note**
>
> AD authentication will break if the account used to read the AD directory becomes invalid (for example, if the account's password is changed or expires or if the account is disabled).

6. Enter the AD domain in the *Default AD Domain* box.

   The domain must be specified as the FULL DOMAIN NAME in ALL CAPS or a child domain name from where most users will be logging onto the BI platform. This should match the default domain specified in the Kerberos configuration files that are used to configure the application server. You can map groups from the default domain without specifying the domain name prefix. If you enter a default AD domain name, users from the default domain do not have to specify the AD domain name when logging onto the BI platform using AD authentication.
7. In the *Mapped AD Member Groups* area, enter the AD domain\group in the *Add AD Group (Domain\Group)* box, using one of the following formats to map groups:
   - Security Account Manager account name (SAM), also referred to as NT name (`DomainName\GroupName`)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

   > **Note**
   >
   > If you want to map a local group, use only the NT name format: `\\<ServerName>\<GroupName>`. AD does not support local users; local users who belong to a mapped local group will not be mapped to the BI platform. Therefore, they cannot access the system.

   > **Tip**
   >
   > When manually logging onto BI launch pad, users from other domains must append the domain name, in uppercase letters, after their user name. For example `CHILD.PARENTDOMAIN.COM` is the domain in
   >
   > ```
   > user@CHILD.PARENTDOMAIN.COM
   > ```
8. Click *Add*.

   The group is added to the list under *Mapped AD Member Groups*.
9. Under *Authentication Options*, select *Use Kerberos authentication*.
10. In the *Service principal name* box, enter the SPN mapped to the service account you created to run BI platform servers.

    > **Note**
    >
    > You must specify the SPN for the service account that runs the SIA. For example: `BICMS/bossosvcacct.domain.com`.
11. Click *Update*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Caution**
>
> Do not proceed if users and/or groups are not mapping in properly! To resolve specific AD group mapping issues refer to SAP note 1631734.

> **Note**
>
> If you have successfully mapped AD group accounts and do not want to configure AD authentication options or AD group updates, skip steps 12 to 19. You can configure these optional settings after you have successfully set up manual AD Kerberos authentication.

12. If your configuration requires SSO to a database, select *Cache security context*.

> **Note**
>
> If this is your initial AD authentication configuration, it is recommended that you first successfully set up manual AD authentication before you consider the extra configuration required for SSO.

13. Select *Enable single sign-on for selected authentication mode* if you require SSO for your AD authentication configuration.
14. In the *Synchronization of Credentials* area, select an option to enable and update the AD user's data source logon credentials .

    This option synchronizes the data source with the user's current logon credentials, thereby enabling scheduled reports to run when the user is not logged on to the BI platform and Kerberos SSO is not available.
15. In the *AD Alias Options* area, specify how new aliases are added to and updated in the BI platform.
    a. In the *New Alias Options* area, select an option for mapping new aliases to Enterprise accounts:
        - *Assign each new AD alias to an existing User Account with the same name*
          Select this option when you know users have an existing Enterprise account with the same name; that is, AD aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and AD account, are added as new users.
        - *Create a new user account for each new AD alias*
          Select this option when you want to create a new account for each user.

    b. In the *Alias Update Options* area, select an option for managing alias updates for the Enterprise accounts:
        - *Create new aliases when the Alias Update occurs*
          Select this option to automatically create a new alias for each AD user mapped to the BI platform. New AD accounts are added for users without BI platform accounts, or for all users if you selected *Create a new user account for each new AD alias* and clicked *Update*.
        - *Create new aliases only when the user logs on*
          Select this option when the AD directory you are mapping contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.

    c. In the *New User Options* area, select an option for creating new users:
        - *New users are created as named users*
          New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the BI platform based on a user name and password.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This provides named users with access to the system, regardless of how many people are connected. You must have a named user license available for each user account created using this option.

- *New users are created as concurrent users*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.

16. To configure how to schedule AD alias updates, click *Schedule*.
    a. In the *Schedule* dialog box, select a recurrence from the *Run object* list.
    b. Set other schedule options and parameters as required.
    c. Click *Schedule*.
    When the alias update occurs, the group information is also updated.
17. In the *Attribute Binding Options* area, specify the attribute binding priority for the AD plugin:
    a. Select the *Import Full Name, Email Address and other attributes* check box.
    The full names and descriptions used in AD accounts are imported and stored with user objects in BI platform.
    b. Specify an option for *Set priority of AD attribute binding relative to other attributes binding*.
    If the option is set to 1, AD attributes take priority when AD and other plugins (LDAP and SAP) are enabled. If the option is set to 3, attributes from other enabled plugins take priority. The bindings must be set to different values. Setting multiple authentication plugins to the same binding value leads to unexpected results.
18. In the *AD Group Options* area, configure AD group updates:
    a. Click *Schedule*.
    The *Schedule* dialog box appears.
    b. Select a recurrence from the *Run object* list.
    c. Set other schedule options and parameters as required.
    d. Click *Schedule*.

    The system schedules the update and runs it according to the schedule you specified. The next scheduled update for the AD group accounts is displayed under the *AD Group Options*.
19. In the *On-Demand AD Update* area, select one of the following options:
    - *Update AD Groups now*
      Select this option if you want to start updating all scheduled AD groups when you click *Update*. The next scheduled AD group update is listed under *AD Group Options*.
    - *Update AD Groups and Aliases now*
      Select this option if you want to start updating all scheduled AD groups and user aliases when you click *Update*. The next scheduled updates are listed under *AD Group Options* and *AD Alias Options*.
    - *Do not update AD Groups and Aliases now*
      No AD groups or user aliases will be updated when you click *Update*.
20. Click *Update*, and click *OK*.

To verify that you have actually imported AD user accounts, go to *CMC* > *User and Groups* > *Group Hierarchy* and select the AD group you have mapped to view users in that group. The current and nested users in the AD group will be displayed.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To create a Kerberos configuration file [page 248]

9.4.3.3 Scheduling updates for Windows AD groups

The BI platform enables administrators to schedule updates for AD groups and user aliases. This feature is available for AD authentication with either Kerberos or NTLM. The CMC also enables you to view the time and date when the last update was performed.

> **Note**
>
> For AD authentication to work on the BI platform, you must configure how updates are scheduled for your AD groups and aliases.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Table 43:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can specify what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will be run on the dates specified in a calendar that has previously been created.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Scheduling AD group updates

The BI platform relies on AD for user and group information. To minimize the volume of queries sent to AD, the AD plugin caches information about groups and how they relate to each other and their user membership. The update does not run when no specific schedule is defined.

You must use the CMC to configure the recurrence of the group update refresh. This should be scheduled to reflect how frequently your group membership information is modified.

Scheduling AD user alias updates

User objects can be aliased to an AD account, allowing users to use their AD credentials to log on to BI platform. Updates to AD accounts are propagated to the BI platform by the AD plug-in. Accounts created, deleted, or disabled in AD will be correspondingly created, deleted, or disabled in the BI platform.

If you do not schedule AD alias updates, updates will occur only when:

- A user logs on; 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.

9.4.4 Configuring the BI platform service to run the SIA

9.4.4.1 Running the SIA under the BI platform service account

To support AD Kerberos authentication for the BI platform, you must grant the service account the right to act as part of the operating system. This must be done on each machine running a Server Intelligence Agent (SIA) with the Central Management Server (CMS).

To enable the service account to run/start the SIA, you must configure specific operating system settings described in this section.

> **Note**
>
> If you will require single sign-on to the database, the SIA must include the following servers:
>
> - Crystal Reports Processing Server
> - Report Application Server
> - Web Intelligence Processing Server

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.4.2 To configure the SIA to run under the service account

Before configuring the SIA account to run under the BI platform service account you must complete the following prerequisite actions:

- A service account has been created on the domain controller for the BI platform.
- You have verified that the required service principal names (SPN) have been added to the service account.
- You have successfully mapped AD user groups into the BI platform.

Perform this task for any Server Intelligence Agent (SIA) that is running services used by the service account.

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

   > **Note**
   >
   > When you stop the SIA, all services managed by the SIA are stopped.

3. Right-click the SIA and select *Properties*.
4. Clear the *System Account* check box.
5. Type the service account credentials (**<DOMAINNAME>\<service name>**) and click *OK*.

   The service account must be granted the following rights on the machine running the SIA:

   - The account must specifically have the “Act as part of operating system” right.
   - The account must specifically have the “Logon as a service” right.
   - Full control rights to the folder where BI platform is installed.
   - Full control rights to “ HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects” in the system registry.
6. Click *Start > Control Panel > Administrative Tools > Local Security Policy*.
7. Expand *Local Policies*, then click *User Rights Assignment*.
8. Double-click *Act as part of the operating system*.
9. Click *Add*, and enter the name of the service account you created, then click *OK*.
10. Repeat the above steps on each machine running a BI platform server.

    > **Note**
    >
    > It is important that the Effective Right ends up being checked after *Act as part of the operating system* is selected. Typically, you will need to restart the server for this to occur. If, after restarting the server, this option is still not on, your Local Policy settings are being overridden by your Domain Policy settings.

11. Restart the SIA.
12. If necessary, repeat steps 1 to 5 for each SIA running a service that must be configured.

You should now be able to login into the CCM using AD credentials.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.4.3 To test AD credentials on the CCM

To perform this task, you need to have successfully mapped an AD user group into the BI platform.

1. Open the CCM and click the *Manage Servers* icon.
2. Ensure that the right information is displayed in the *System* field.
3. Select *Windows AD* from the authentication options list.
   A login dialog box opens.
4. Log on using an existing AD account from the AD group you mapped into the BI platform.

> **Note**
>
> If you are using an AD account that does not reside in the default domain, login as `domain\username`.

You should not receive any error messages. You must be able to log in via the CCM using a mapped AD account before moving to the next section.

> **Tip**
>
> If you get an error message, go to *CMC* > *Authentication* > *Windows AD*. Under *Authentication Options*, change *Use Kerberos authentication* to *Use NTLM authentication* and click *Update*. Repeat steps 1-4 above. If this works, there is an issue with your Kerberos configuration.

9.4.5 Configuring the web application server for AD Authentication

9.4.5.1 Preparing the application server for Windows AD authentication (Kerberos)

The process of configuring Kerberos for a web application server varies slightly depending on the specific application server. However, the general process of configuring Kerberos involves these steps:

- Creating the Kerberos `(krb5.ini)` configuration file.
- Creating the JAAS login `bscLogin.conf` configuration file.

> **Note**
>
> This step is not required for the SAP NetWeaver 7.3 Java application server. However you will need to add the LoginModule to your SAP NetWeaver server.

- Modifying the Java options for your application server.
- Overwriting the `BOE.war` file properties for Windows AD authentication.
- Restarting your Java application server.

This section contains the details for configuring Kerberos for use with the following application servers:

- Tomcat

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 Creating Kerberos configuration files

9.4.5.1.1.1 To create a Kerberos configuration file

Before proceeding, ensure you have performed the following prerequisite tasks:

- A service account has been created on the domain controller for the BI platform.
- You have verified that the service principal names (SPNs) have been added to the service account.
- You have successfully mapped AD user groups into the BI platform.
- You have tested AD credentials on the CCM.

Follow these steps to create the Kerberos configuration file if you're using SAP NetWeaver 7.3, Tomcat, Oracle Application Server, WebSphere, or WebLogic as the web application server for your BI platform deployment.

1. Create the file `krb5.ini`, if it does not exist, and store it under `C:\Windows` for Windows.

   > **Note**
   >
   > If the application server is installed on Unix, you should use the following directories:
   >
   > Solaris: `/etc/krb5/krb5.conf`
   >
   > Linux: `/etc/krb5.conf`

   > **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. 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
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

Note

The key parameters are explained in the table below.

Table 44:

`DOMAIN.COM`	The DNS name of your domain which must be entered in uppercase in FQDN format.
`kdc`	The Host name of the Domain Controller.
`[capath]`	Defines the trust between domains that are in another AD forest. In the example above `DOMAIN2.COM` is a domain in an external forest and has direct two way transitive trust to `DOMAIN.COM`.
`default_realm`	In a multiple domain configuration, under `[libdefaults]` the `default_realm` value may be any of the source domains. The best practice is to use the domain with the greatest number of users that will be authenticating with their AD accounts. If no UPN suffix is supplied at log on, it defaults to the value of `default_realm`. This value should be consistent with the *default domain* setting in the CMC. All domains must be specified in uppercase as shown in the example above.

9.4.5.1.2 Creating a JAAS login configuration file

9.4.5.1.2.1 To create a Tomcat or WebLogic JAAS login configuration file

The `bscLogin.conf` file is used to load the java login module and is required for AD Kerberos authentication on Java web application servers.

The default location for the files is: `C:\Windows`.

1. Create a file called `bscLogin.conf` if it does not exist, and store it in `C:\Windows`.

Note

You can store this file in a different location. However, if you do, you will need to specify its location in your java options.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Add the following code to your JAAS `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Save and close the file.

9.4.5.1.2.2 To create an Oracle JAAS login configuration file

1. Locate the `jazn-data.xml` file.

> **Note**
>
> The default location for this file is `C:\OraHome_1\j2ee\home\config`. If you installed Oracle Application Server in a different location, find the file specific to your installation.

2. Add the following content to the file between the `<jazn-loginconfig>` tags:

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Save and close the `jazn-data.xml` file.

9.4.5.1.2.3 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:\Windows`
2. Add the following code to your `bscLogin.conf` configuration file:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Save and close the file.

9.4.5.1.2.4 To add a LoginModule to SAP NetWeaver AS

To use Kerberos and SAP NetWeaver AS 7.3, configure the system as if you were using the Tomcat web application server. You will not need to create a `bscLogin.conf` file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Once this has been done, you need to add a LoginModule and update some Java settings on SAP NetWeaver AS 7.3.

To map the `com.sun.security.auth.module.Krb5LoginModule` to the `com.businessobjects.security.jgss.initiate`, you need to manually add a LoginModule to SAP NetWeaver AS 7.3.

1. Open the SAP 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*.
   SAP 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 you 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 SAP NetWeaver Administrator.

9.4.5.1.3 Modifying the application server Java settings to load configuration files

9.4.5.1.3.1 To modify the Java options for Kerberos on Tomcat

1. From the *Start* menu, select *Programs >Tomcat > Tomcat Configuration*.
2. Click the *Java* tab.
3. Add the following options:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

   Replace XXXX with the location where you stored the `bscLogin.conf` file.
4. Close the Tomcat configuration file.
5. Restart Tomcat.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.5.1.3.2 To modify the Java options for SAP NetWeaver AS 7.3

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 SAP NetWeaver AS (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* and add the following custom parameter information:

java.security.krb5.conf	**<path to the krb5.ini file including the file name>**
javax.security.auth.useSubjectCredsOnly	false

8. Click *Save*, and then click *Configuration Editor*.
9. Click *Configurations* > *Security* > *Configurations* > *com.businessobjects.security.jgss.initiate* > *Security* > *Authentication*.
10. Click *Edit Mode*.
11. Right-click the *Authentication* node and select *Create sub-node*.
12. Select *Value-Entry* from the top list.
13. Enter the following:

Name	create_security_session
Value	false

14. Click *Create* and then close the window.
15. Click *Config Tool* and then*Save*.

Once you have updated your configuration, you need to restart your SAP NetWeaver AS.

9.4.5.1.3.3 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 WebLogic domain that runs your BI platform applications.
2. Open the script that starts the domain of WebLogic that runs your BI platform applications (`startWeblogic.cmd` for Windows, `startWebLogic.sh` for Unix).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.security.krb5.conf=C:/XXX/krb5.ini
```

   Replace XXXX with the location you stored the file.
4. Restart the domain of WebLogic that runs your BI platform applications.

9.4.5.1.3.4 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 onto the administration console of your Oracle Application Server.
2. Click the name of the OC4J instance that runs your BI platform 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.

9.4.5.1.3.5 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 the BI platform.
3. Go to the *JVM* page.

   If you are using WebSphere 5.1, follow these steps to get to the *JVM* page.

   1. On the server page, scroll down until you see *Process Definition* in the *Additional Properties* column.
   2. Click *Process Definition*.
   3. Scroll down and click *Java Virtual Machine*.

   If you are using WebSphere 6.0, follow these steps to get to the *JVM* page.

   1. On the server page, select *Java and Process Management*.
   2. Select *Process Definition*.
   3. Select *Java Virtual Machine*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Click *Generic JVM arguments* then specify the location of your `Krb5.ini` and the location of your `bscLogin.conf` file as shown below.

   -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.

9.4.5.1.4 To verify that Java can receive a Kerberos ticket

Before testing if Java has received the Kerberos ticket, you must complete the following prerequisite actions:

- Create the `bscLogin.conf` file for your application server.
- Create the `krb5.ini` file.

1. Go to the command prompt and navigate to the `jdk\bin` directory in your BI platform installation.

   By default this is located in:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.
2. Run `kinit <username>`.
3. Press `Enter`.
4. Type the password.
   If the `krb5.ini` file was configured properly and the Java login module has been loaded, you should see the following message:
   New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator

Do not continue with the AD setup until you have successfully received a Kerberos ticket.

If you cannot receive a ticket, consider the following options:

- Consult the troubleshooting section at the end of this chapter.
- For issues concerning the KDC, the Kerberos configuration files, and user credentials not available in the Kerberos database, refer to SAP Knowledge Base articles KBA 1476374 and KBA 1245178.

9.4.5.1.5 To configure BI launch pad for manual AD login

Before configuring your BI platform applications for manual AD login, the following prerequisite actions must be completed:

- You have created a service account on the domain controller for the BI platform.
- You have verified that the HTTP service principal names (SPN) have been added to the service account.
- You have successfully mapped AD user groups into the BI platform.
- You have tested AD credentials on the CCM.
- You have created, configured, and tested the required configuration files for your web application server.
- Your application server's Java settings have been modified to load the configuration files.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

To enable the Windows AD authentication option for both BI launch pad, perform the following steps:

1. Access the custom folder for the BOE web application on the machine hosting the web application server: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Make your changes in the `config\custom` and not the `config\default` directory. Otherwise your changes will be overwritten when future patches will be applied to your deployment.

   You will have to later redeploy the modified BOE web application.
2. Create a new file.

   > **Note**
   >
   > Use Notepad or any other text-editing utility.
3. Save the file as `BIlaunchpad.properties`.
4. Type the following:

   ```
   authentication.visible=true
   authentication.default=secWinAD
   ```
5. Save and close the file.
6. Restart your web application server.

You should now be able to manually log into BI launch pad. Access either application and select Windows AD from the list of authentication options.

> **Note**
>
> Do not continue with your Windows AD setup until you can manually log into BI launch pad with an existing AD account.

The new properties will take effect only after the BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy BOE on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

> **Note**
>
> If your deployment uses a firewall, remember to open all the required ports; otherwise, the web applications will not be able to connect to the BI platform servers.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.6 Single Sign-On Setup

9.4.6.1 SSO to the BI platform with AD authentication

Options for SSO using Windows AD

There are two supported methods for setting up single sign-on (SSO) for Windows AD authentication with the BI platform:

- Vintela - this option can only be used with Kerberos.
- SiteMinder - this option can only be used with Kerberos.

SSO to the database

SSO to the database enables logged-on users to perform actions that require database access, in particular, viewing, and refreshing reports, without having to provide their logon credentials again. While constrained delegation is optional for AD authentication and Vintela SSO, it is required for deployment scenarios that involve single sign-on to the system database.

End-to-end SSO

In the BI platform, end-to-end SSO is supported through Windows AD and Kerberos. In this scenario, users have both single sign-on access to the BI platform at the front-end, and SSO access to the databases at the back-end. Thus, users need to provide their logon credentials only once, when they log on to the operating system, to have access to the BI platform and to be able to perform actions that require database access, such as viewing reports.

Manual versus SSO AD authentication configuration

Once you have successfully configured your deployment to enable AD accounts to manually log into BI launch pad, you need to revisit the AD authentication setup to enable specific SSO requirements. Requirements will vary depending on your choice of SSO method.

9.4.6.2 Using Vintela SSO

9.4.6.2.1 Checklist for Vintela SSO setup

To set up the BI platform to work with Vintela SSO, you need to complete the following tasks:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Specifically configure your service account for Vintela SSO.
2. Configure constrained delegation (optional).
3. Configure the Windows AD SSO authentication options in the CMC.
4. Configure the general and BI launch pad-specific properties for Vintela SSO.
5. If you are using Tomcat as the web application server for your deployment, you need to increase the header size limit.
6. Configure the internet browsers for Vintela.

9.4.6.2.2 To set up the service account for Vintela SSO

The `Ktpass` command-line tool configures the server principal name for the host or service in Active Directory and generates a Kerberos "keytab" file containing the shared secret key of the service account. This tool is usually found on domain controllers or it can be downloaded from the Microsoft support site: http://support.microsoft.com/kb/892777 .

You need a service account specifically configured to allow users in a given Windows AD group to automatically authenticate to BI launch pad with their AD credentials. You can reconfigure the service account created for AD Kerberos authentication on the domain controller.

When a client attempts log into BI launch pad, a request to the Kerberos ticket-generating server is initiated. To facilitate this request, the service account created for the BI platform must have an SPN that matches the URL of the application server. Perform the following steps on the machine hosting the domain controller.

1. Run the Kerberos keytab setup command `ktpass` to create and place a `keytab` file.

   Specify the `ktpass` parameters listed in the following table:

   Table 45:

Parameter	Description
-out	Specifies the name of the Kerberos `keytab` file to generate.
-princ	Specifies the principal name used for the service account, in SPN format:**< MYSIAMYSERVER>**/**<sbo.service.domain.com>**@**<DOMAIN>.**COM, where **<MYSIAMYSERVER>** is the name of the Service Intelligence Agent as specified in the Central Configuration Manager (CCM). **Note** The name of your service account is case-sensitive. The SPN includes the name of the host computer on which the service instance is running. **Tip** The SPN must be unique in the forest in which it is registered. To check, use the Windows support tool `Ldp.exe` to search for the SPN.
-pass	Specifies the password used by the service account.
-ptype	Specifies the principal type: `-ptype KRB5_NT_PRINCIPAL`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description
-crypto	Specifies the encryption type to use with the service account: `-crypto RC4-HMAC-NT`

For example:

```
ktpass -out <keytab_filename>.keytab -princ <MYSIAMYSERVER>/
sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

The output from the `ktpass` command should confirm the target domain controller and that a Kerberos `keytab` file containing the shared secret was created. The command also maps the principal name to the (local) service account.

2. Right-click the service account, select *Properties* > *Delegation*.
3. Click *Trust this user for delegation to any service (Kerberos only)*.
4. Click *OK* to save your settings.

The service account now has all the required service principal names for Vintela SSO and you have generated a keytab file with the encrypted password for the service account.

9.4.6.2.2.1 To configure constrained delegation for Vintela SSO

Constrained delegation is optional for setting up Vintela SSO. It is, however, mandatory for deployments that require SSO 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 in the previous section, and click *Properties* > *Delegation*.
3. Select *Trust this user for delegation to the specified services only*.
4. Select *Use Kerberos only*.
5. Click *Add* > *Users or Computers*.
6. Type the service account name and click *OK*.
   A list of services is displayed.
7. Select the following services and then click *OK*.
   - The HTTP service
   - The service used to run the Service Intelligence Agent (SIA) on the machine hosting the BI platform.

   The services are added to the list of services that can be delegated for the service account.

You will need to modify the web application properties to account for this modification.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.6.2.3 To configure SSO settings in the CMC

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Ensure the *Enable Windows Active Directory (AD)* check box is selected.
4. Under *Authentication Options*, ensure the *Use Kerberos authentication* option is selected.
5. If your configuration requires SSO to the database, select *Cache security context*.
6. Select *Enable single sign-on for selected authentication mode*.
7. Click *Update*.

9.4.6.2.4 To enable Vintela single sign-on for BI launch pad and OpenDocument

This procedure is used for either BI launch pad or OpenDocument. To enable SSO to the BI platform web applications, you need to specify Vintela and SSO-specific properties in the `BOE.war` file. For SSO setup purposes, it is recommended that you concentrate on enabling SSO to BI launch pad for AD accounts before handling other applications.

1. Access the custom folder for the BOE web application on the machine hosting the web application server:
   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Make your changes in the `config\custom` directory and not the `config\default` directory. Otherwise your changes will be overwritten when future patches will be applied to your deployment.

   You will have to later redeploy the modified BOE web application.
2. Create a new file using a text editor.
3. Enter the following:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
idm.logger.props=error-log.properties
```

> **Note**
>
> The idm.realm and idm.princ parameters require valid values. The idm.realm should be the same value you set when you configured the `default_realm` in your `krb5.ini` file. The value must be in upper case. The idm.princ parameter is the SPN used for the service account created for Vintela SSO.

> **Note**
>
> Forward slashes are required when specifying the keytab file location.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Skip the following step if you do not want to use constrained delegation for Windows AD authentication and Vintela SSO.

4. To use constrained delegation, add:

```
idm.allowS4U=true
```

5. Close the file and save it with a `global.properties` name.

> **Note**
>
> Make sure the file name is not saved under any extensions such as `.txt`.

6. Create another file in the same directory. Save the file as `OpenDocument.properties` or `BIlaunchpad.properties` depending on your requirements.
7. Type the following:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

For example:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

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

The new properties will take effect only after the BOE web application is redeployed on the machine running the web application server. Use WDeploy to redeploy BOE on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

> **Note**
>
> If your deployment is using a firewall, remember to open all the required ports otherwise the web applications will not be able to connect to the BI platform servers.

9.4.6.2.5 To enable Vintela single sign-on for Web Services

Some client tools will require authentication through web services. Follow these steps to enable single sign-on (SSO) for web services.

1. Back up this file: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml` and then open it for editing.
2. Uncommment the Kerberos Proxy Filter and Kerberos Filter sections to enable Kerberos SSO for Windows Active Directory (secWinAD) authentication.

   The following options must be specified (the rest are optional):

   - `idm.realm` (the same as the default_realm specified in the Krb5.ini file).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- idm.princ (the same as specified for idm.princ in the global.properties file located at **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom).
- idm.keytab (the same as specified for idm.keytab in the global.properties file located at **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom).

> **Note**
>
> If you are using the hardcoded password set in Tomcat's Java Options, do not make any changes to the keytab lines in the web.xml file.

3. If SSL is not in use with the Java application server, then set the idm.allowUnsecured parameter to **true**.

   For more information about Tomcat SSL, see the Knowledge Base Article ID:1484802.
4. Back up this file: **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties and open it for editing.
5. Set kerberos.sso to **true** and save the file.
6. Use WDeploy to redeploy the WAR file on the web application server.

   For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
7. Restart Tomcat.
8. To test your settings, on the client machine with client tools installed, launch Query as a Web Service Designer.
9. Add a new Managed Host.
10. Enter the application server name.
11. Enter the Web Services URL in this format: http://<WebAppServer>:<portNumber>/dswsbobje/services/Session.

    Example: http://BI4:8080/dswsbobje/services/Session.
12. Enter the CMS hostname.
13. Change the Authentication type to *Windows AD*.
14. Select *Enable Windows Active Directory Single Sign On*.
15. At the login prompt, leave the *User* and *Password* fields blank and click *OK*.

9.4.6.2.6 To increase the header size limit for Tomcat

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 the BI platform on Windows, and you did not modify the default

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

installation location, replace `<TomcatINSTALLDIR>` with `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\`

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

2. Find the corresponding `<Connector ...>` tag for the port number you have configured.

   If you are using the default port of 8080, find the `<Connector ...>` tag with port="8080" in it.

   For example:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. Add the following value within the `<Connector ...>` tag:

   `maxHttpHeaderSize="16384"`

   For example:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080" redirectPort="8443" />
```

4. Save and close the `server.xml` file.
5. Restart Tomcat.

> **Note**
>
> For other Java application servers, consult your Java application server's documentation.

9.4.6.2.7 Configuring Internet browsers

To support Vintela SSO for AD Kerberos authentication, you must configure BI platform clients. This involves configuring the web browser on the client machines.

9.4.6.2.7.1 To configure Internet Explorer on the client machines

1. On the client machine, open an IE browser.
2. Enable integrated Windows authentication.
   a. On the *Tools* menu, click *Internet Options*.
   b. Click the *Advanced* tab.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

c. Scroll to *Security*, select *Enable Integrated Windows Authentication*, and then click *Apply*.

3. Add the Java Application machine or the URL to the trusted sites. You can enter the full domain name of the site.
   a. On the *Tools* menu, click *Internet Options*.
   b. Click the *Security* tab.
   c. Click *Sites* and then click *Advanced.*
   d. Select or enter the site and click *Add.*
   e. Click *OK* until the Internet Options dialog box closes.
4. Close and reopen the Internet Explorer browser window for these changes to take effect.
5. Repeat all of these steps on each BI platform client machine.

9.4.6.2.7.2 To configure Firefox on the client machines

1. *Modify network.negotiate-auth.delegation-uris*
   a. On the client machine, open a Firefox browser.
   b. Type **about:config** in the URL address field.
      A list of configurable properties appears.
   c. Double-click *network.negotiate-auth.delegation-uris* to edit the property.
   d. Enter the URL that you will use to access BI launch pad.

      For example if your BI launch pad URL is **http://<machine.domain.com>:8080/BOE/BI**, then you need to enter **http://<machine.domain.com>**.

      > **Note**
      >
      > To add more than one URL, separate them with a comma. For example: **http://<machine.domain.com>,<machine2.domain.com>**.

   e. Click *OK*.
2. *Modify network.negotiate-auth.trusted-uris*
   a. On the client machine, open a Firefox browser.
   b. Type **about:config** in the URL address field.
      A list of configurable properties appears.
   c. Double-click *network.negotiate-auth.trusted-uris* to edit the property.
   d. Enter the URL that you will use to access BI launch pad. .
      For example if your BI launch pad URL is **http://<machine.domain.com>:8080/BOE/BI**, then you will need to enter **http://<machine.domain.com>**

      > **Note**
      >
      > To add more than one URL, separate them with a comma. For example: **http://<machine.domain.com>,<machine2.domain.com>**.

   e. Click *OK*.
3. Close and reopen the Firefox browser window for these changes to take effect.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Repeat all of these steps on each BI platform client machine.

9.4.6.2.8 Testing Vintela SSO for AD Kerberos authentication

You should test your SSO setup from a client workstation. Make sure that the client is on the same domain as your BI platform deployment, and that you are logged into the workstation as a mapped AD user. This user account must be able to manually log into BI launch pad.

To test SSO, open a browser and enter the URL for BI launch pad. If SSO is properly configured, you should not be prompted for your logon credentials.

➡ Tip

It is recommended that you test various AD user scenarios in your deployment. For example, if your environment will have users from multiple operating systems, you should test SSO for users from each operating system. You should also test SSO against all the possible browsers supported in your organization. If your environment will have users from multiple forests or domains, you should test SSO for a user account from each domain or forest.

9.4.6.2.9 Configuring Kerberos and single sign-on to the database for application servers

Single sign-on to the database is supported for deployments that meet all these requirements:

- The deployment of the BI platform is on a web application server.
- The web application server has been configured for Vintela SSO for AD authentication.
- The database to which SSO is required is a supported version of SQL Server or Oracle.
- The groups or users that need access to the database must have been granted permissions within SQL Server or Oracle. .

The final step is to modify the `krb5.ini` file to support SSO to the database for web applications.

9.4.6.2.9.1 To enable single sign-on to the database for Java application servers

1. Open the `krb5.ini` file that is being used for your deployment of the BI platform.

   The default location for this file is the WIN directory on your web application server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> If you cannot find the file in the WIN directory, check this Java argument for the location of the file:
>
> ```
> -Djava.security.auth.login.config
> ```
>
> This variable is specified when AD with Kerberos is configured on your web application server.

2. Go to the `[libdefaults]` section of the file.
3. Enter this string prior to the start of the `[realms]` section of the file:

   ```
   forwardable=true
   ```
4. Save and close the file.
5. Restart your web application server.

Single sign-on to the database will not be enabled until you check the *Cache security context (required for SSO to database)* box in the Windows AD authentication page in the CMC.

9.4.6.3 Using SiteMinder

9.4.6.3.1 Using Windows AD with SiteMinder

This section explains how to use AD and SiteMinder. SiteMinder is a third-party user access and authentication tool that you can use with the AD security plug-in to create single sign-on to the BI platform. You can use SiteMinder with Kerberos.

Ensure your SiteMinder identity management resources are installed and configured before configuring Windows AD authentication to work with SiteMinder. For more information about SiteMinder and how to install it, refer to your SiteMinder documentation.

There are two tasks you must complete to enable AD single sign-on with SiteMinder:

- Configure the AD plug-in for single sign-on with SiteMinder
- Configure SiteMinder properties for the BOE web application

> **Note**
>
> Ensure that the SiteMinder Administrator has enabled support for 4.x Agents. This must be done regardless of which supported version of SiteMinder you are using. For more information about SiteMinder configuration, refer to your SiteMinder documentation.

9.4.6.3.1.1 To enable SiteMinder properties for BI launch pad

In addition to specifying SiteMinder settings for the Windows AD security plugin, SiteMinder settings must be specified for the BOE war properties.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Locate the **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\ directory in your BI platform installation.
2. Create a new file in the directory, using Notepad or another text-editing utility.
3. In the new file, enter the following values:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Save the file with the name `global.properties`.

> **Note**
>
> Make sure the file name is not saved with an extension, such as `.txt`.

5. Create another file in the same directory.
6. In the new file, enter the following values:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

For example:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Save the file with the name `BIlaunchpad.properties`, and close the file.

The new properties take effect after BOE.war is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

9.4.6.3.1.2 To configure SiteMinder settings in the CMC

Before configuring the CMC for SiteMinder, you must complete the following prerequisite actions:

- You have successfully mapped AD user groups into the BI platform.
- You have tested AD credentials on the CCM.

1. Go to the *Authentication* management area of the CMC.
2. Double-click *Windows AD*.
3. Select the *Enable Windows Active Directory (AD)* check box.
4. Under Authentication Options, select *Use NTLM authentication* or *Use Kerberos authentication*.

   To configure the BI platform for Kerberos and AD authentication using Kerberos, you must have a service account. You can either create a new domain account or use an existing domain account. The service account will be used to run BI platform servers.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Tip**
>
> When manually logging on to BI launch pad, users from other domains must append the domain name, in uppercase letters, after their user name. For example, in `user@CHILD.PARENTDOMAIN.COM`, "CHILD.PARENTDOMAIN.COM" is the domain.

5. If you selected *Use Kerberos authentication*:
   a. If you want to configure single sign-on to a database, select *Cache security context*.
   b. Delete any information in the *Service principal name* box.
6. If you want to configure single sign-on, select *Enable Single Sign On for selected authentication mode*.

   You must also configure BOE web application general properties and BI launch pad properties to enable single sign-on.
7. In the *Synchronization of Credentials* area, select an option to enable and update the AD user's data source credentials at logon.

   This option synchronizes the data source with the user's current logon credentials.
8. In the *SiteMinder Options* area, configure SiteMinder as your single sign-on option for AD authentication using Kerberos:
   a. Click *Disabled.*

      The *Windows Active Directory* page appears.

      If you have not configured the Windows AD plug-in, a warning appears, asking if you want to continue. Click *OK*.
   b. Click *Use SiteMinder Single Sign On*.
   c. In the *Policy Server Host* box, type the name of each policy server, and click *Add*.
   d. For each policy server host, enter a port number in the *Accounting*, *Authentication*, and *Authorization* boxes.
   e. In the *Agent Name* box, enter the agent name.
   f. In the *Shared Secret* boxes, enter the shared secret.

      Ensure that the SiteMinder Administrator has enabled support for 4.x Agents, regardless of which supported version of SiteMinder you use. For information about SiteMinder and how to install it, see the SiteMinder documentation.
   g. Click *Update* to save and return to the main AD authentication page.
9. In the *AD Alias Options* area, specify how new aliases are added to and updated in the BI platform.
   a. In the *New Alias Options* area, select an option for mapping new aliases to Enterprise accounts:
      - *Assign each new AD alias to an existing User Account with the same name*
        Select this option when you know users have an existing Enterprise account with the same name; that is, AD aliases will be assigned to existing users (auto alias creation is turned on). Users who do not have an existing Enterprise account, or who do not have the same name in their Enterprise and AD account, are added as new users.
      - *Create a new user account for each new AD alias*
        Select this option when you want to create a new account for each user.
   b. In the *Alias Update Options* area, select an option for managing alias updates for the Enterprise accounts:
      - *Create new aliases when the Alias Update occurs*
        Select this option to automatically create a new alias for each AD user mapped to the BI platform. New AD accounts are added for users without BI platform accounts, or for all users if you selected *Create a new user account for each new AD alias* and clicked *Update*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- *Create new aliases only when the user logs on*
  Select this option when the AD directory you are mapping contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to the BI platform.

c. In the *New User Options* area, select an option for creating new users:

- *New users are created as named users*
  New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on a user name and password. This provides named users with access to the system, regardless of how many people are connected. You must have a named user license available for each user account created using this option.
- *New users are created as concurrent users*
  New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users.

10. To configure how to schedule AD alias updates, click *Schedule*.
    a. In the *Schedule* dialog box, select a recurrence from the *Run object* list.
    b. Set other schedule options and parameters as required.
    c. Click *Schedule*.
    When the alias update occurs, the group information is also updated.
11. In the *Attribute Binding Options* area, specify the attribute binding priority for the AD plugin:
    a. Select the *Import Full Name, Email Address and other attributes* check box.
    The full names and descriptions used in AD accounts are imported and stored with user objects in the BI platform.
    b. Specify an option for *Set priority of AD attribute binding relative to other attributes binding*.
    If the option is set to 1, AD attributes take priority when AD and other plugins (LDAP and SAP) are enabled. If the option is set to 3, attributes from other enabled plugins take priority. The bindings must be set to different values. Setting multiple authentication plugins to the same binding value leads to unexpected results.
12. In the *AD Group Options* area, configure AD group updates:
    a. Click *Schedule*.
    The *Schedule* dialog box appears.
    b. Select a recurrence from the *Run object* list.
    c. Set other schedule options and parameters as required.
    d. Click *Schedule*.

    The system schedules the update and runs it according to the schedule you specified. The next scheduled update for the AD group accounts is displayed under the *AD Group Options*.
13. In the *On-Demand AD Update* area, select an option to indicate whether to update AD groups or users (or neither) when you click *Update*:

- *Update AD Groups now*
  Select this option if you want to start updating all scheduled AD groups when you click *Update*. The next scheduled AD group update is listed under *AD Group Options*.
- *Update AD Groups and Aliases now*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Select this option if you want to start updating all scheduled AD groups and user aliases when you click *Update*. The next scheduled updates are listed under *AD Group Options* and *AD Alias Options*.

- *Do not update AD Groups and Aliases now*
  No AD groups or user aliases will be updated when you click *Update*.

14. Click *Update*, and click *OK*.

9.4.6.3.1.3 To disable SiteMinder

If you want to prevent SiteMinder from being configured, or to disable it after it has been configured in the CMC, modify the web configuration file for BI launch pad.

9.4.6.3.1.3.1 To disable SiteMinder for Java clients

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 BI platform installation:
   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Open the `global.properties` file.
3. Change siteminder.enabled to false

   ```
   siteminder.enabled=false
   ```

4. Save your changes and close the file.

The change takes effect only after `BOE.war` is redeployed on the machine running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

9.4.7 Troubleshooting Windows AD authentication

9.4.7.1 Troubleshooting your configuration

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Java SDK Kerberos configuration

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.4.7.1.1 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\<user name>\.businessobjects\jce_verbose.log
```

9.4.7.1.2 To test your Kerberos configuration

Run the following command to test your Kerberos configuration, where `servant` is the service account and domain under which the CMS is running, and `password` is the password associated with the service account.

```
<InstallDirectory>\SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin
\servact@TESTM03.COM Password
```

For example:

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\
 servact@TESTM03.COM Password
```

Your domain and service principal name must exactly match the domain and service principal name in the Active Directory. If the problem persists, check whether you entered the same name; note that the name is case-sensitive.

9.4.7.1.3 Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to the BI platform. Despite this fact, they are unable to successfully log onto the CMC or BI launch pad with Windows AD authentication and Kerberos in the following format: `DOMAIN\ABC123`

This problem can happen when the user is set up in Active Directory with a UPN and SAM name that are not exactly the same. The following examples may cause a problem:

- The UPN is abc123@company.com but the SAM name is DOMAIN\ABC123.
- The UPN is jsmith@company but the SAM name is DOMAIN\johnsmith.

There are two ways to address this problem:

- Have users log in using the UPN name rather than the SAM name.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Ensure the SAM account name and the UPN name are the same.

9.4.7.1.4 Pre-authentication error

A user who has previously been able to log on, can no longer log on successfully. The user will receive this error: Account Information Not Recognized. The Tomcat error logs reveal the following error: `"Pre-authentication information was invalid (24)"`

This can occur because the Kerberos user database didn't get a change made to UPN in AD. This may mean that the Kerberos user database and the AD information are out of sync.

To resolve this problem, reset the user's password in AD. This will ensure the changes are propagated correctly.

> **Note**
>
> This problem is not an issue with J2SE 5.0.

9.5 SAP authentication

9.5.1 Configuring SAP authentication

This section explains how to configure BI platform authentication for your SAP environment.

SAP authentication enables SAP users to log on to the BI platform using their SAP user names and passwords, without storing passwords in the BI platform. SAP authentication also allows you to preserve information about user roles in SAP and to use role information in the platform to assign rights for performing administrative tasks or accessing content.

Accessing the SAP authentication application

You must provide the BI platform with information about your SAP system. A dedicated web application is accessible through the main BI platform administration tool, the Central Management Console (CMC). To access it from the home page of the CMC, click *Authentication*.

Authenticating SAP users

Security plug-ins expand and customize the ways in which the BI platform authenticates users. The SAP Authentication feature includes an SAP security plug-in (`secSAPR3.dll`) for the Central Management Server (CMS) component of the BI platform. This SAP security plug-in offers several key benefits:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- It acts as an authentication provider that verifies user credentials against your SAP system on behalf of the CMS. When users log on to the BI platform directly, they can choose SAP Authentication and provide their usual SAP user name and password. The BI platform can also validate Enterprise Portal logon tickets against SAP systems.
- It facilitates account creation by allowing you to map roles from SAP to BI platform user groups, and it facilitates account management by allowing you to assign rights to users and groups in a consistent manner within the BI platform.
- It dynamically maintains SAP role listings. So, once you map an SAP role to the platform, all users who belong to that role can log on to the system. When you make subsequent changes to the SAP role membership, you need not update or refresh the listing in the BI platform.
- The SAP Authentication component includes a web application for configuring the plug-in. You can access this application in the *Authentication* area of the Central Management Console (CMC).

9.5.2 Creating a user account for the BI platform

The BI platform system requires an SAP user account that is authorized to access SAP role membership lists and authenticate SAP. You will need the account credentials to connect the BI platform 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 by setting values for the following authorization objects:

Table 46:

Authorization object	Field	Value
Authorization for file access (S_DATASET)	Activity (ACTVT)	Read, Write (33, 34)
	Physical file name (FILENAME)	* (denotes All)
	ABAP program name (PROGRAM)	*
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)
User Master Maintenance: User Groups (S_USER_GRP)	Activity (ACTVT)	Create or Generate, and Display (03)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Value
	User group in user master maintenance (CLASS)	* **Note** For greater security, you may prefer to explicitly list the user groups whose members require access to the BI platform.

Finally, add the `CRYSTAL` user to the `CRYSTAL_ENTITLEMENT` role.

Tip

If your system policies require users to change their passwords when they first log onto the system, log on now with the `CRYSTAL` user account and reset its password.

9.5.3 Connecting to SAP entitlement systems

Before you can import roles or publish BW content to the BI platform, you must provide information about the SAP entitlement systems to which you want to integrate. The BI platform uses this information to connect to the target SAP system when it determines role memberships and authenticates SAP users.

9.5.3.1 To add an SAP entitlement system

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link.

   The entitlement systems settings appear.

   Tip

   If an entitlement system is already displayed in the *Logical system name* list, click *New*.
3. In the *System* field, type the three-character System ID (SID) of your SAP system.
4. In the *Client* field, type the client number that the BI platform must use when it logs on to your SAP system. The BI platform combines your System and Client information, and adds an entry to the *Logical system name* list.
5. Ensure the *Disabled* check box is clear.

   Note

   Use the *Disabled* check box to indicate to the BI platform that a particular SAP system is temporarily unavailable.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Complete the *Message Server* and *Logon Group* fields as appropriate, if you have set up load balancing such that the BI platform must log on through a message server.

   > **Note**
   >
   > You must make the appropriate entries in the `Services` file on your BI platform machine to enable load balancing - especially if your deployment not on a single machine. Specifically you should account for the machines hosting the CMS, the Web application server, as well as all machines managing your authentication accounts and settings.

7. If you have not set up load balancing (or if you prefer to have the BI platform log on directly to the SAP system), complete the *Application Server* and *System Number* fields as appropriate.
8. In the *User name*, *Password*, and *Language* fields, type the user name, password, and language code for the SAP account that you want the BI platform to use when it logs on to SAP.

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

9. Click *Update*.

If you add multiple entitlement systems, click the *Options* tab to specify the system that the BI platform uses as the default (that is, the system that is contacted to authenticate users who attempt to log on with SAP credentials but without specifying a particular SAP system).

Related Information

Creating a user account for the BI platform [page 272]

9.5.3.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.5.3.3 To temporarily disable a connection to an SAP entitlement system

In the CMC, you can temporarily disable a connection between the BI platform and an SAP entitlement system. This may be useful to maintain the responsiveness of the BI platform in cases such as the scheduled down time of an SAP entitlement system.

1. In the CMC, go to the *Authentication* management area.
2. Double-click the *SAP* link.
3. In the *Logical system name* list, select the system you want to disable.
4. Select the *Disabled* check box.
5. Click *Update*.

9.5.4 Setting SAP Authentication options

SAP Authentication includes a number of options that you can specify when integrating the BI platform with your SAP system. The options include:

- Enabling or disabling SAP authentication
- Specifying connection settings
- Linking imported users to BI platform license models.
- Configuring single sign-on to the SAP system

9.5.4.1 To set SAP Authentication options

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link, and click the *Options* tab.
3. Review and modify the following settings as needed:

Setting	Description
Enable SAP Authentication	Clear this check box to disable SAP Authentication. **Note** To disable SAP Authentication for a specific SAP system, select that system's *Disabled* check box on the *Entitlement Systems* tab.
Content folder root	Specify where the BI platform should begin replicating the BW folder structure in the CMC and in BI launch pad. The default is `/SAP/2.0`, but you can change it to a different folder. If you want to change the value, you must

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Description
	change it both in the CMC and Content Administration Workbench.
Default system	Select a SAP entitlement system for the BI platform to contact to authenticate users who attempt to log on with SAP credentials but without specifying a particular SAP system. **Note** If you select a default system, users from that system do not have to enter a system ID or client when connecting from client tools, like Live Office or Universe Designer, using SAP authentication. For example, if SYS~100 is set as the default system, SYS~100/user1 could log on as user1 when SAP authentication is chosen.
Max. number of failed attempts to access entitlement system	Type the number of times that the BI platform should attempt to contact an SAP system to fulfill authentication requests. Setting the value to -1 allows the platform to attempt to contact the entitlement system an unlimited number of times. Setting the value to 0 limits the BI platform to making one attempt to contact the entitlement system. **Note** Use this setting with the *Keep entitlement system disabled [seconds]* option to configure how the BI platform handles SAP entitlement systems that are temporarily unavailable. The system uses the two options to determine when to stop communicating with an SAP system that is unavailable and when to resume communication with that system.
Keep entitlement system disabled [seconds]	Type the number of seconds for the BI platform to wait before resuming attempts to authenticate users against the SAP system. For example, if *Max failed entitlement system accesses* is set to 3, the BI platform allows a maximum of three failed attempts to authenticate users against any SAP system. A fourth failed attempt stops the system from attempting to authenticate users against that system for the amount of time specified.
Max. concurrent connections per system	Specify how many connections to keep open in your SAP system at the same time. For example, if you type 2, the BI platform keeps two connections open to SAP.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Description
Number of uses per connection	Specify how many operations to allow to the SAP system per connection. For example, if *Max concurrent connections per system* is set to 2 and *Number of uses per connection* is set to 3, once there are three logons on one connection, the BI platform closes and restarts that connection.
Concurrent users and *Named users*	Specify whether new user accounts will use concurrent user licenses or named user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small number of concurrent licenses can support a large user base. For example, depending on how often and how long users access the system, a 100-user concurrent license could support 250, 500, or 700 users. Named user licenses are associated with users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. **Note** The option you select does not change the number or type of user licenses installed in the BI platform. You must have the appropriate licenses available on your system.
Import Full Name, Email Address and other attributes	Specify a priority level for the SAP authentication plugin. The full names and descriptions used in the SAP accounts are imported and stored with user objects in the BI platform.
Set priority of SAP attribute binding relative to other attributes binding	Specifies a priority for binding SAP user attributes (full name and email address). If the option is set to 1, SAP attributes take priority in scenarios where SAP and other plugins (Windows AD and LDAP) are enabled. If the option is set to 3, attributes from other enabled plugins will take priority. The bindings must be set to different values. Setting multiple authentication plugins to the same binding value leads to unexpected results.

Set the following options to configure the SAP single sign-on service:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Description
System ID	The system identifier provided by the BI platform to the SAP system when performing the SAP single sign-on service.
Browse	Click to upload the `keystore` file generated to enable the SAP single sign-on. You can also manually enter the full path to the file.
Key Store Password	Provide the password required to access the `keystore` file.
Private Key Password	Provide the password required to access the certificate corresponding to the `keystore` file. The certificate is stored on the SAP system
Private Key Alias	Provide the alias required to access the `keystore` file.

4. Click *Update*.

Related Information

Configuring SAP authentication [page 271]

9.5.4.2 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 the BI platform to begin replicating the BW folder structure from.
4. Click *Update*.
5. In the BW Content Administration Workbench, expand *Enterprise system*.
6. Expand *Available systems* and double-click the system that the BI platform is connecting to.
7. Click the *Layout* tab and in the *Content base folder*, type the folder that you want to use as the root SAP folder in the BI platform (for example, `/SAP/2.0/`).

9.5.5 Importing SAP roles

By importing SAP roles into the BI platform, you allow role members to log onto the system with their usual SAP credentials. In addition, single sign-on is enabled so that SAP users are logged on to the BI platform automatically when they access reports from within the SAP GUI or an SAP Enterprise Portal.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> There are often many requirements for enabling SSO. Some of these might include using a driver and application that are SSO-capable, and ensuring your server and web server are in the same domain.

For each role that you import, the BI platform generates a group. Each group is named with the following convention: **<SystemID~ClientNumber@NameOfRole>**. You can view the new groups in the *Users and Groups* management area of the CMC. You can also use these groups to define object security within the BI platform.

Consider three main categories of users when configuring the BI platform for publishing, and when importing roles to the system:

- BI platform administrators
  Enterprise administrators configure the system for publishing content from SAP. They import the appropriate roles, create necessary folders, and assign rights to those roles and folders in the BI platform.
- Content publishers
  Content publishers are those users who have rights to publish content into roles. The purpose of this category of user is to separate regular role members from those users with rights to publish reports.
- Role members
  Role members are users who belong to "content bearing" roles. That is, these users belong to roles to which reports are published. They have *View*, *View on Demand*, and *Schedule* rights for any reports published to the roles they are members of. However, regular role members cannot publish new content, nor can they publish updated versions of content.

You must import all content publishing and all content bearing roles to the BI platform prior to publishing for the first time.

> **Note**
>
> It is strongly recommended that you keep the activities of roles distinct. For example, while it is possible to publish from an administrator role, it is better practice to publish only from content publisher roles. Additionally, the function of content publishing roles is only to define which users can publish content. Thus, content publishing roles should not contain any content; content publishers should publish to content bearing roles that are accessible to regular role members.

Related Information

How rights work in BI platform [page 112]
Managing security settings for objects in the CMC [page 120]

9.5.5.1 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 *Concurrent users* or *Named users*, depending on your license agreement.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This option does not change the number or type of user licenses that you have installed in the BI platform. You must have the appropriate licenses available on your system.

4. Click *Update*.
5. On the *Role Import* tab, select the appropriate entitlement system from the *Logical system name* list.
6. In the *Available roles* area, select the role(s) that you want to import, and click *Add*.
7. Click *Update*.

9.5.5.2 To verify that roles and users were imported correctly

Before starting this task, take note of the user name and password of an SAP user who belongs to one of the roles that you mapped to the BI platform.

1. For Java BI launch pad, go to **`http://<webserver>:<portnumber>/BOE/BI`**.

   Replace **`<webserver>`** with the name of the web server and **`<portnumber>`** with the port number for the BI platform. You may need to ask your administrator for the name of the web server, the port number, or the URL to enter.
2. From the *Authentication Type* list, select *SAP*.

   > **Note**
   >
   > By default, the *Authentication Type* list is hidden in BI launch pad. If the list is not visible, ask your system administrator to enable the *Authentication Type* list in the `BIlaunchpad.properties` file and then restart the app server.

3. Enter the SAP system and system client that you want to log on to.
4. Enter the user name and password of a mapped user.
5. Click *Log On*.

   You are logged on to BI launch pad as the selected user.

9.5.5.3 Updating SAP roles and users

After enabling SAP authentication, it is necessary to schedule and run regular updates on mapped roles that have been imported into the BI platform. This will ensure that your SAP role information is accurately reflected in the platform.

There are two options for running and scheduling updates for SAP roles:

- Update roles only: using this option will only update the links between the currently mapped roles that have been imported in the BI platform. It is recommended that you use this option if you expect to run frequent updates, and you have concerns over system resource usage. No new user accounts will be created if you only update SAP roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in the BI platform for user aliases added to roles in the SAP system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

9.5.5.3.1 To schedule updates for SAP roles

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

1. Click the *User Update* tab.
2. Click *Schedule* in the *Update Roles Only* section or the *Update Roles and Aliases* area.

   > **Tip**
   >
   > To immediately run an update, click *Update Now*.

   > **Tip**
   >
   > Use the *Update Roles Only* option if you would like frequent updates and have concerns about system resources. It takes the system longer to update both roles and aliases.

   The *Recurrence* dialog box appears.
3. Select an option from the *Run Object* list and provide all the requested scheduling information in the fields provided.

   When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

   Table 47:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify the time it will start and the start and end dates.
Daily	The update will run every day or every **<n>** days (where **<n>** is the number of days you specify). You can specify the time it will start and the start and end dates.
Weekly	The update will run every week, once a week or several times a week. You can specify on which days it will run, the time it will start, and the start and end dates.
Monthly	The update will run every month or every several months. You can specify the time it will start and the start and end dates.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as and a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as and a start and end date.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 and a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule*.
   The date of the next scheduled role update appears on the *User Update* tab.

> **Tip**
>
> To cancel the next scheduled update, click *Cancel Scheduled Updates* in the *Update Roles Only* area or *the Update Roles and Aliases* area.

9.5.6 Configuring Secure Network Communication (SNC)

This section describes how to configure SNC as part of the process of setting up SAP authentication to the BI platform

Before setting up trust between the SAP and BI platform systems, you must ensure the SIA is configured to start and run under an account that has been set up for SNC. You must also configure your SAP system to trust the BI platform.

Related Information

SAP Server-Side Trust Overview [page 282]

9.5.6.1 SAP Server-Side Trust Overview

This section provides procedures for configuring server-side trust between SAP Web Application Servers (version 6.20 and up) and SAP BusinessObjects Business Intelligence platform. You need to set up server-side trust if you are using multi-pass report bursting (for publications where the report query depends on the context of the user).

Server-side trust involves password-less impersonation. To impersonate an SAP user without providing a password, a user must be identified with SAP using a more secure method than a regular username and password. (An SAP user with the `SAP_ALL` authorization profile cannot impersonate another SAP user without knowing that user's password.)

Enabling server-side trust using the SAP crypto library

To enable server-side trust for the BI platform using the SAP Cryptographic Library, you must run the relevant servers under credentials that are authenticated using a registered Secure Network Communication (SNC)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

provider. These credentials are configured within SAP to be allowed to impersonate without a password. For the BI platform, you need to run the servers involved in report-bursting under these SNC credentials, such as the Adaptive Job Server.

You need 32-bit SNC binaries for 32-bit processes; 64-bit SNC binaries for 64-bit processes. An SAP Cryptographic Library is installed along with the BI platform. Note that the SAP Cryptographic Library can be used only for setting up server-side trust. The Cryptographic Library is available for Windows and UNIX.

For more information about the Cryptographic Library, see SAP notes 711093, 597059 and 397175 on the SAP web site.

The SAP server and the BI platform need to be assigned certificates that prove their identities to each other. Each server will have its own certificate and a list of certificates for trusted parties. To configure server-side trust between SAP and the BI platform, you need to create a password-protected set of certificates called a Personal Security Environment (PSE). This section describes how to set up and maintain the PSEs, and how to securely associate them with BI platform processing servers.

Client versus server SNC

In client SNC, an SNC name identifier is mapped to one (or more) SAP user names in SU01. When a logon request is sent, the SNC name together with the SAP name is passed to the SAP system; however, no password is sent. If the SNC name maps to the specified SAP name, the logon is permitted. A client-side logon string for a direct application host logon is shown below:

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN USER=USER123
SNC_MODE=1 SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US"
```

The SAP user USER123 must be mapped to `p:CN=TheUser, O=TheCompany, C=US in SU01` for this logon attempt to succeed. In server SNC on the other hand, it is not a requirement to explicitly map between the SNC name identifier and SAP user name. Instead, the SNC name is configured in transaction `SNC0` to be allowed to perform an impersonation-style logon for “any” user without having to provide this user's password. For example:

```
 ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN SNC_MODE=1
SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US" EXTIDTYPE=UN EXTIDDATA=USER123
```

The server SNC impersonation logon, or logon via external ID is much more powerful than its client counterpart. This logon enables access to any SAP user account in the system. Other External ID logon options include Logon Tickets and X.509 client certificates.

SAP BusinessObjects BI platform server responsibilities

Specific BI platform servers are relevant to the SAP integration in terms of single sign-on (SSO). The following table lists these servers, and the type of SNC they require for particular areas of responsibility.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Server	SNC type	Areas of responsibility
Web Application Server	client	SAP Authentication role list
BW Publisher Service	server	Crystal Reports Dynamic Parameter pick lists and personalization
CMS	client	Password, ticket, checking role membership, and user lists
Page Server	server	Crystal Reports view on demand
Job Server	server	Scheduling Crystal Reports
Web Intelligence Processing Server	server	Viewing and scheduling Web Intelligence reports and List of Values (LOV) prompts
Multi-Dimensional Analysis Service	server	Analysis

> **Note**
>
> The Web Application Server and the CMS use client-SNC and thus require an explicit mapping of the SNC name to the SAP user name. This is specified in either transaction `SU01` or `SM30` for table `USRACL`.

9.5.6.2 Configuring SAP for server-side trust

Server-side trust applies only to Crystal reports and Web Intelligence reports that are based on Universes (`.unv`). You must set up SNC for use with the BI platform. For more information or for troubleshooting assistance, consult the SAP documentation provided with your SAP server.

9.5.6.2.1 To configure SAP for server-side trust

1. Ensure that you have SAP administrator's credentials for within SAP and for the machine running SAP, and administrator's credentials for the BI platform and the machine (or machines) it is running on.
2. On the SAP machine, ensure that the SAP Cryptographic Library and the SAPGENPSE tool are located in the `<DRIVE>:\usr\sap\<SID>\SYS\exe\run\` directory (on Windows).
3. Create an environment variable named **`<SECUDIR>`** that points to the directory where the ticket resides.

   > **Note**
   >
   > This variable must be accessible to the user under which SAP's *disp+work* process runs.

4. In the SAP GUI, go to transaction RZ10 and change the instance profile in *Extended maintenance* mode.
5. In profile edit mode, point SAP profile variables to the Cryptographic Library and give the SAP system a Distinguished Name (DN). These variables should follow the LDAP naming convention:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Tag	Meaning	Description
`CN`	Common Name	The everyday name of the certificate proprietor.
`OU`	Organizational Unit	PG for Product Group, for example.
`O`	Organization	The name of the organization for which the certificate was issued.
`C`	Country	The country where the organization is located.

For example, for R21: `p:CN=R21, OU=PG, O=BOBJ, C=CA`

> **Note**
>
> The prefix `p:` is for the SAP Cryptographic Library. It is required when referring to the DN within SAP, but will not be visible when examining certificates in STRUST or using SAPGENPSE.

6. Enter the following profile values, substituting for your SAP system where necessary:

Profile variable	Value
`ssf/name`	`SAPSECULIB`
`ssf/ssfapi_lib`	Full path to sapcrypto lib
`sec/libsapsecu`	Full path to sapcrypto lib
`snc/gssapi_lib`	Full path to sapcrypto lib
`snc/identity/as`	Your SAP system's DN

7. Restart your SAP instance.
8. When the system is running again, log on and go to transaction STRUST, which should now have additional entries for SNC and SSL.
9. Right-click the SNC node and click *Create*.
   The identity you specified in RZ10 should now appear.
10. Click *OK*.
11. To assign a password to the SNC PSE, click the lock icon.

> **Note**
>
> Do not lose this password. You will be prompted for it by STRUST every time you view or edit the SNC PSE.

12. Save the changes.

> **Note**
>
> If you do not save your changes, the application server will not start again when you enable SNC.

13. Return to transaction RZ10 and add the remainder of the SNC profile parameters:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Profile variable	Parameter
`snc/accept_insecure_rfc`	`1`
`snc/accept_insecure_r3int_rfc`	`1`
`snc/accept_insecure_gui`	`1`
`snc/accept_insecure_cpic`	`1`
`snc/permit_insecure_start`	`1`
`snc/data_protection/min`	`1`
`snc/data_protection/max`	`3`
`snc/enable`	`1`

The minimum protection level is set to authentication only (1) and the maximum is privacy (3). The `snc/data_protection/use` value defines that only authentication is to be used in this case, but could also be (2) for integrity, (3) for privacy and (9) for maximum available. The `snc/accept_insecure_rfc`, `snc/accept_insecure_r3int_rfc`, `snc/accept_insecure_gui`, and `snc/accept_insecure_cpic` values set to (1) ensure that previous (and potential unsecure) communication methods are still permitted.

14. Restart your SAP system.

You must now configure the BI platform for server-side trust.

9.5.6.3 Configuring the BI platform for server-side trust

The following procedures need to be performed in order to configure the BI platform for server-side trust. Note that these steps are Windows-based, but because the SAP tool is a command line tool, the steps are very similar on Unix.

1. Set up the environment
2. Generate a Personal Security Environment (PSE)
3. Configure the BI platform servers
4. Configure PSE access
5. Configure SAP Authentication SNC settings
6. Set up SAP dedicated server groups

Related Information

To set up the environment [page 287]
To generate a PSE [page 287]
To configure BI platform servers [page 288]
To configure PSE access [page 289]
To configure SAP authentication SNC settings [page 290]
Using server groups [page 290]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.5.6.3.1 To set up the environment

The BI platform includes a default SAP Cryptographic Library. If you use the default library, you need to perform only the last two steps: create a subfolder, and add an environment variable. Otherwise, to configure a custom copy of the SAP Cryptographic Library, perform all of the steps.

The default SAP Cryptographic Library can be found at this location:

- Windows: **<INSTALLDIR>**\sap\sapcrypto.dll
- Unix: **<INSTALLDIR>**/sap/libsapcrypto.so

Before you begin, ensure that:

- The SAP Cryptographic Library has been expanded on the host on which BI platform processing servers run.
- The appropriate SAP systems have been configured to use SAP Cryptographic Library as the SNC provider.

Before PSE maintenance can begin, you need to set up the library, tool, and environment where PSEs are stored.

1. Copy the SAP Cryptographic Library (including the PSE maintenance tool) to a folder on the machine running the BI platform.

   For example: `C:\Program Files\SAP\Crypto`
2. Add the folder to the **<PATH>** environment variable.
3. Add a system-wide environment variable **<SNC_LIB>** that points to the Cryptographic Library.

   For example: `C:\Program Files\SAP\Crypto\sapcrypto.dll`

   > **Note**
   >
   > The maximum path length is 100 characters.
4. Create a subfolder named **sec**.

   For example: `C:\Program Files\SAP\Crypto\sec`
5. Add a system-wide environment variable **<SECUDIR>** that points to the **sec** folder.

Related Information

Configuring SAP for server-side trust [page 284]

9.5.6.3.2 To generate a PSE

SAP accepts a BI platform server as a trusted entity when the relevant BI platform servers have a PSE and the PSE is associated with SAP. This “trust” between SAP and BI platform components is established by sharing the public version of each other's certificates. The first step is to generate a PSE for the BI platform that automatically generates its own certificate.

1. Open a command prompt and run **sapgenpse.exe gen_pse -v -p BOE.pse** from within the Cryptographic Library folder.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Choose a PIN and the DN you want for your BI platform system.

   For example, **CN=MyBOE01, OU=PG, O=BOBJ, C=CA**.

   You now have a default PSE, with its own certificate.
3. Use the following command to export the certificate in the PSE:

   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
4. In the SAP GUI, go to transaction STRUST and open the system PSE associated with your SAP system.

   You may be prompted for the password you have already assigned to this system PSE.
5. Import the **<MyBOECert.crt>** file created earlier by clicking the "Import Certificate" button at the bottom left of the STRUST transaction screen.

   The certificates from SAPGENPSE are Base64-encoded. Make sure you select Base64 when importing them.
6. To add the BI platform certificate to the SAP server's PSE certificate list, click the *Add to certificate list* button.
7. Save your changes in STRUST.
8. Click the *Export* button and provide a file name for the certificate.

   For example, **MySAPCert.crt**.

   > **Note**
   >
   > The format should remain Base64.
9. Go to transaction SNC0.
10. Add a new entry, where:
    - The System ID is arbitrary but reflects your BI platform system.
    - The SNC name should be the DN (prefixed by **p:**) that you provided when you created your BI platform PSE (in step 2).
    - The *Entry for RFC activated* and *Entry for ext. ID activated* check boxes are both selected:
11. To add the exported certificate to the BI platform PSE, run the following command on the command prompt:

    sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse

The SAP Cryptographic Library is installed on the BI platform machine. You have created a PSE that will be used by BI platform servers to identify themselves to SAP servers. SAP and the BI platform PSE have exchanged certificates. SAP permits entities with access to the BI platform PSE to perform RFC calls and password-less impersonation.

Related Information

To configure BI platform servers [page 288]

9.5.6.3.3 To configure BI platform servers

After you generate a PSE for the BI platform, you must configure an appropriate server structure for SAP processing. The following procedure creates a node for SAP processing servers, so that you can set operating system credentials on the node level.

 © 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> In this version of the BI platform, servers are no longer configured in the Central Configuration Manager (CCM). Instead, a new Server Intelligence Agent (SIA) must be created.

1. In the CCM, create a new node for SAP processing servers.

   Give the node an appropriate name such as **SAPProcessor**.
2. In the CMC, add the processing servers you need to the new node, then start the new servers.

9.5.6.3.4 To configure PSE access

After you configure the BI platform node and servers, you need to configure PSE access using the SAPGENPSE tool.

1. Run the following command from the command prompt:

   ```
   sapgenpse.exe seclogin -p SBOE.pse
   ```

   > **Note**
   >
   > You will be prompted for the PSE PIN. If you run the tool under the same credentials used by your BI platform SAP processing servers, you do not need to specify a user name.
2. To verify that the single sign-on (SSO) link is established, list the contents of the PSE using the following command:

   ```
   sapgenpse.exe maintain_pk -l
   ```

   The results should look similar to the following:

   ```
   C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:\Documents and Settings\username\My Documents\snc\sec
   \bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***

   1. ------------------------------------------------------------
              Version:                 0 (X.509v1-1988)
              SubjectName:             CN=R21Again, OU=PG, O=BOBJ, C=CA
              IssuerName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
              SerialNumber:            00
              Validity  -  NotBefore:  Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                  NotAfter:    Thu
   Dec 31 16:00:01 2037 (3801010000001Z)
              Public Key Fingerprint:  851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
              SubjectKey:              Algorithm RSA (OID 1.2.840.113549.1.1.1),
   NULL


   C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
   ```

   You should not be prompted again for the PSE PIN after a successful **seclogin** command.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> If you encounter PSE access problems, use the -O argument to specify PSE access. For example, to grant PSE access to a specific user in a specific domain, on Windows, type this command:
>
> ```
> sapgenpse seclogin -p SBOE.pse -O SYSTEM
> ```

9.5.6.3.5 To configure SAP authentication SNC settings

After you configure PSE access, you must configure SAP authentication settings in the CMC.

1. Go to the *Authentication* management area of the CMC.
2. Double-click the *SAP* link.

   The entitlement systems settings appear.
3. Click the *SNC Settings* tab on the *SAP Authentication* page.
4. Select your entitlement system from the *Logical system name* list.
5. Select *Enable Secure Network Communication (SNC)* under *Basic Settings*.
6. Select the *Use Default* option to accept the default path for the library, or select the *Define Custom Path* option to choose a different location.
7. Select a level of protection under *Quality of Protection*.

   For example, select *Authentication*.

   > **Note**
   >
   > Do not exceed the level of protection configured on the SAP system. The level of protection is customizable and is determined by your organization's needs and the capabilities of their SNC library.
8. Enter the SNC name of the SAP system under *Mutual authentication settings*.

   The SNC name format depends on the SNC library. Using the SAP cryptography library, the distinguished name recommendation is that it follows LDAP naming conventions and has `p:` as its prefix.
9. Confirm that the SNC name of the credentials under which the BI platform servers run appears in the *SNC name of Enterprise system* box.

   When several SNC names are configured, this field should be left blank.
10. Provide the DNs of the SAP system and the BI platform PSE.

9.5.6.3.6 Using server groups

Unless the processing (Crystal Reports or Web Intelligence) servers are running under credentials that have access to the PSE, you must create a specific server group containing only these servers along with the required supporting servers. For more information and descriptions of the various BI platform servers, see the “Architecture” chapter.

There are three options to choose from when configuring content processing servers for your SAP content:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Maintain a single SIA, including all BI platform servers, running under credentials that have access to the PSE. This is the simplest option - no server groups need to be created. This approach is the least secure in that an unnecessary number of servers have access to the PSE.
2. Create a second SIA with access to the PSE and add to it the Crystal Reports or Web Intelligence processing servers. Delete the duplicated servers from the original SIA. No server groups need to be created but fewer servers have access to the PSE.
3. Create a SIA exclusively for use for SAP with access to the PSE. Add to it the Crystal Reports or Web Intelligence processing servers. With this option, only SAP content should run on these servers, and more importantly, SAP content should run only on these servers. Since in this scenario content needs to be directed to certain servers, you must create server groups for the SIA.

Guidelines for using a server group

The server group needs to reference the SIA used exclusively to handle SAP content. In addition, the server group needs to reference the following servers:

- Adaptive Servers
- Adaptive Job Servers

All SAP content, Web Intelligence documents, and Crystal reports need to be associated with the server group using the strictest association; that is, that they must run on servers in the group. When this association is done on an object level, the server group setting should be propagated into settings for both direct scheduling as well as for publications.

To prevent other (non-SAP) content from processing on the SAP-specific processing servers, you should create another server group that includes all the servers under the original SIA. It is recommended that you set up a strict association between this content and the non-SAP server group.

9.5.6.4 Configuring multi-pass publications

Troubleshooting multi-pass publications

If you encounter problems with multi-pass publications, enable tracing for the Crystal Reports (CR) or Multidimensional Data Access (MDA) drivers for SAP and look at the logon string used for each job or recipient. These logon strings should resemble the following:

```
 SAP: Successfully logged on to SAP server.
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:\WINDOWS\System32\sapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3
EXTIDTYPE=UN
```

The logon string must have the appropriate **EXTIDTYPE=UN** (for username) and **EXTIDDATA** should be the SAP username of the recipient. In this example, the logon attempt was successful.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.5.6.5 Workflow for integrating with Secure Network Communication

The BI platform supports environments that implement Secure Network Communication (SNC) for authentication and data encryption between SAP components. If you have deployed the SAP Cryptographic Library (or another external security product that uses the SNC interface) you must set some additional values to integrate the BI platform effectively within your secured environment.

To configure the platform to use your secure network communication, you must complete the following tasks:

1. Configure BI platform servers to start and run under an appropriate user account.
2. Configure the SAP system to trust your BI platform system.
3. Configure the SNC settings in the SNC link in the Central Management Console.
4. Import SAP roles and users into the BI platform.

Related Information

Importing SAP roles [page 278]
Configuring SAP for server-side trust [page 284]
Configuring the BI platform for server-side trust [page 286]

9.5.6.6 To configure SNC settings in the Central Management Console

Before you can configure SNC settings, you must add a new entitlement system to the BI platform, ensure that the SNC library file is in a known directory, and create an environment variable **<RFC_LIB >**to point to the file.

1. Click the *SNC Settings* tab on the *SAP Authentication* page.
2. Select your entitlement system from the *Logical system name* list.
3. Select *Enable Secure Network Communication (SNC)* under *Basic Settings*.
4. If you are configuring SAP authentication for the consumption of `.unx` Universes or OLAP BICS connections and plan to use STS, select the *Prevent insecure incoming RFC connections* check box.
5. Select the *Use Default* option to accept the default path for the library, or select the *Define Custom Path* option to choose a different location.

   The application server and the CMS must be on the same OS type with the same path to the crypto library.
6. Select a level of protection under *Quality of Protection*.

   For example, select *Authentication*.

> **Note**
>
> The level of protection is customizable and is determined by your organization's needs and the capabilities of their SNC library.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

7. Enter the SNC name of the SAP system under *Mutual authentication settings*.

   The SNC name format depends on the SNC library. Using the SAP cryptography library, the distinguished name recommendation is that it follows LDAP naming conventions and has `p:` as its prefix.
8. Confirm that the SNC name of the credentials under which BI platform servers run appears in the *SNC name of Enterprise system* box.

   When several SNC names are configured, leave this box blank.
9. Click *Update.*
10. Click the *Entitlement systems* tab on the *SAP Authentication* page.
    The *SNC name* option appears under the *Language* option.
11. In the *SNC name* box, enter the SNC name that you configured on the SAP BW server.

    The name should be the same as the name used to configure the SAP system to trust the BI platform.

    If you are using the Insight to Action Framework to enable the Report-to-Report Interface, it may take up to 10 minutes before SNC is enabled or for changes to SNC settings to take effect. To trigger an immediate update, restart the Adaptive Processing Server that is running the Insight to Action Service.

Related Information

Connecting to SAP entitlement systems [page 273]

9.5.6.7 To associate the entitlement user with an SNC name

1. Log on to your SAP BW system and execute the transaction `SU01`.

   The User Maintenance: Initial Screen opens.
2. In the *User* field, type the name of the SAP account designated as the entitlement user and then click *Change* on the toolbar.

   The Maintain User screen opens.
3. Click the SNC tab.
4. In the *SNC name* field, type the `SNC USER ACCOUNT` you entered in step 2 above.
5. Click *Save*.

9.5.6.8 To add a system ID to the SNC Access Control list

1. Log on to your SAP BW system and execute the transaction `SNC0`.

   The Change View "SNC: Access Control List (ACL) for Systems: Overview" screen opens.
2. Click *New Entries* on the toolbar.

   The New Entries: Details of Added Entries screen opens.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Type the name of your BI platform machine in the *System ID* field.
4. Type `p:<SNC USER NAME>` in the *SNC user name* field, where `SNC USER NAME` represents the account you used when configuring the BI platform servers.

> **Note**
>
> If your SNC provider is gssapi32.dll, use uppercase letters when indicating the SNC USER NAME. You must include the domain name when specifying the user account. For example: domain\username.

5. Select *Entry for RFC activated* and *Entry for ext. ID activated*.
6. Clear all other options and click *Save*.

9.5.7 Setting up single sign-on to the SAP system

Different BI platform client and back-end services interact with SAP NetWeaver ABAP back-end systems in an integrated environment. It is useful to set up single sign-on from the BI platform to these (typically BW) back-end systems. After an ABAP system is configured as an external authentication system, proprietary SAP tokens are used to provide a mechanism that supports single sign-on for all BI platform clients and services connecting to SAP NetWeaver ABAP systems.

To enable single sign-on to the SAP system, you need to create a `keystore` file and a corresponding certificate. Use the `keytool` command line program to generate the file and the certificate. By default the keytool program is installed in the `sdk/bin` directory for each platform.

The certificate needs to be added to your SAP ABAP BW system, and to the BI platform using the CMC.

> **Note**
>
> The SAP authentication plugin must be configured before you can set up single sign-on to the database used by SAP BW.

9.5.7.1 To generate the keystore file

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

9.5.7.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

You now have a keystore file and a certificate in the directory where the keytool program is located.

9.5.7.3 Importing the certificate file into the target ABAP SAP system

You need a key store file and an associated certificate for your BI platform 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* check box is selected.
5. Click the file path button to point to the location where the certificate file is located.
6. Click the green check mark.
   The certificate file is uploaded.
7. Click *Add to Certificate List*.
   The certificate is displayed in the Certificate List.
8. Click *Add to ACL* and specify a SystemID and Client.

   The system ID must be the same used to identify the BI platform system to SAP BW.

   The certificate is added to the Access Control List (ACL). The client should be specified as “000”.
9. Save your setting and exit.
   The changes are saved in the SAP system.

9.5.7.4 To set up single sign-on to the SAP database in the CMC

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 the System ID for your BI platform system in the field provided.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This should be identical to the value used when importing the certificate in the target SAP ABAP system.

4. Click the *Browse* button to point to the key store file.
5. Provide the following required details:

Field	Required information
Key Store Password	Provide the password required to access the key store file. This password was specified when creating the key store file.
Private Key Password	Provide the password required to access the certificate corresponding to the key store file. This password was specified when creating the certificate for the key store file.
Private Key Alias	Provide the alias required to access the key store file. This alias was specified when creating the key store file.

6. Click *Update* to submit your settings.
   Once the settings are submitted successfully, the following message is displayed under the SystemID field: Key store file have been uploaded

9.5.7.5 To add the Security Token Service to the Adaptive Processing Server

In a clustered environment, Security Token Services are added separately to each Adaptive Processing Server.

1. Go to the *Servers* management area of the CMC.
2. Double-click *Core Services*.
   The list of servers appears under *Core Services*.
3. Right-click the Adaptive Processing Server and select *Stop Server*.

   Do not proceed until the server state is Stopped.
4. Right-click the Adaptive Processing Server and select *Select Services*.
   The *Select Services* dialog box appears.
5. Use the *add* button to move Security Token Service from the *Available services* list to the *Services* list.
6. Click *OK*.
7. Restart the Adaptive Processing Server.

9.5.8 Configuring SSO for SAP Crystal Reports and SAP NetWeaver

By default, the BI platform will be configured to allow SAP Crystal Reports users to access SAP data using Single Sign-on (SSO).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.5.8.1 To deactivate SSO for SAP NetWeaver and SAP Crystal Reports

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select one of the following drivers:

   Table 48:

Driver	Display name
Operational Data Store driver	*crdb_ods*
Open SQL driver	*crdb_opensql*
Infoset driver	*crdb_infoset*
BW MDX Query driver	*crdb_bwmdx*

5. Click *Remove*.
6. Click *Save & Close*.
7. Restart SAP Crystal Reports.

9.5.8.2 To reactivate SSO for SAP NetWeaver and SAP Crystal Reports

Follow the steps below to reactivate SSO for SAP NetWeaver (ABAP) and SAP Crystal Reports.

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Under *Use SSO context for database logon* type:

`crdb_ods`	To activate the ODS driver
`crdb_opensql`	To activate the Open SQL driver
`crdb_bwmdx`	To activate the SAP BW MDX Query driver
`crdb_infoset`	To activate the InfoSet driver

5. Click *Add*.
6. Click *Save & Close*.
7. Restart SAP Crystal Reports.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.6 PeopleSoft authentication

9.6.1 Overview

To use your PeopleSoft Enterprise data with the BI platform, you must provide the program with information about your deployment. This information allows the BI platform to authenticate users so that they can use their PeopleSoft credentials to log on to the program.

9.6.2 Enabling PeopleSoft Enterprise authentication

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

9.6.2.1 To enable PeopleSoft Enterprise authentication in the BI platform

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Double-click *PeopleSoft Enterprise*.
   The *PeopleSoft Enterprise* page appears. It has four tabs: *Options*, *Domains*, *Roles*, and *User Update*.
4. On the *Options* tab, select the *Enable PeopleSoft Enterprise Authentication* check box.
5. Make appropriate changes under *New Alias*, *Update Options*, and *New User Options* according to your BI platform deployment.

   Click *Update* to save your changes before proceeding to the *Domains* tab.
6. Click the *Domains* tab.
7. In the *PeopleSoft Enterprise System User* area, type a database User name and Password for the BI platform to use to log on to your PeopleSoft Enterprise database.
8. In the *PeopleSoft Enterprise Domains* area, enter the Domain name and QAS address used to connect to your PeopleSoft Enterprise environment, and click *Add*.

   > **Note**
   >
   > If you have multiple PeopleSoft domains, repeat this step for any additional domains you want to have access to. The first domain you enter will become the default domain.
9. Click *Update* to save your changes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.6.3 Mapping PeopleSoft roles to the BI Platform

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

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in the BI platform.

Doing so reduces the number of accounts that are created for the same user in the BI platform.

For example, if you run PeopleSoft HR 8.3 and PeopleSoft Financials 8.4, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in the BI platform.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

For example, if you run PeopleSoft HR 8.3 with a user account for Russell Aquino (user name "raquino"), and you run PeopleSoft Financials 8.4 with a user account for Raoul Aquino (user name "raquino"), then you need to create a separate account for each user's alias. Otherwise, the two users are added to the same BI platform account; they will be able to log in to the BI platform with their own PeopleSoft credentials and have access to data from both PeopleSoft systems.

9.6.3.1 To map a PeopleSoft role to the BI Platform

If the BI platform JVM (Java virtual machine) does not have a certificate to the PeopleSoft server, you will need to perform these additional steps before the main steps below:

1. Get the .cer file from the PeopleSoft server.
2. Copy the .cer file to **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Execute the following command from the security directory: `"`**<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file `**<peoplesoftserver>**`.cer -keystore cacerts -alias `**<peoplesoftserver>**.
4. Restart the web application server.

Main steps:

1. Log on as an administrator to the Central Management Console.
2. Click *Authentication*.
3. Double-click *PeopleSoft Enterprise*.
4. On the *Roles* tab, in the PeopleSoft Enterprise Domains area, select the domain associated with the role you want to map to the BI platform.
5. Use one of the following options to select the roles you want to map:
   - In the *PeopleSoft Enterprise Roles* area, in the Search roles box, enter the role you want to locate and map to the BI platform, and then click >.
   - From the *Available Roles* list, select the role you want to map to the BI platform and click >.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> When searching for a particular user or role, you can use the wild card %. For example, to search for all roles beginning with "A," type *A%*. Search is also case sensitive.

> **Note**
>
> If you want to map a role from another domain, you must select the new domain from the list of available domains to match a role from a different domain.

6. Go to the *User Update* tab and either click the *Update* button, or schedule the updates.
7. On the *Options* tab, go to the *New User Options* area and select one of the following options:
   - *Assign each added alias to an account with the same name*
     Select this option if you run multiple PeopleSoft Enterprise systems with users who have accounts on more than one system (and no two users have the same user name for different systems).
   - *Create a new account for every added alias*
     Select this option if you run only one PeopleSoft Enterprise, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.
8. In the *Alias Update Options* area, select one of the following options:
   - *Create new aliases when the Alias Update occurs*
     Select this option to create a new alias for every user that is mapped to the BI platform. New accounts are added for users without the BI platform accounts or for all users if you selected the Create a new account for every added alias option.
   - *Create new aliases only when the user logs on*
     Select this option if the role that you want to map contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to the BI platform for the first time. This is the default option.
9. In the *New User Options* area specify how new users are created.

   Select one of the following options:
   - *New users are created as named users.*
     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.
   - *New users are created as concurrent users.*
     New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the BI platform, a 100 user concurrent license could support 250, 500, or 700 users.

   The roles that you selected now appear as groups in the BI platform.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.6.3.2 Remapping consideration

If you add users to a role that has already been mapped to the BI platform, you need to remap the role to add the users to the BI platform. When you remap the role, the option to map users as either named users or concurrent users affects only the new users that you added to the role.

For example, you first map a role to the BI platform with the "New users are created as *named* users" option selected. Later, you add users to the same role and remap the role with the "New users are created as *concurrent* users" option selected.

In this situation, only the new users in the role are mapped to the BI platform as concurrent users; the users that were already mapped remain named users. The same condition applies if you first map users as concurrent users, and then you change the settings to remap new users as named users.

9.6.3.3 To unmap a role

1. Log on as an administrator to the Central Management Console.
2. Click *Authentication*.
3. Click *PeopleSoft Enterprise*.
4. Click *Roles.*
5. Select the role that you want to remove, and click <.
6. Click *Update*.

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

   > **Note**
   >
   > You can also delete individual accounts or remove users from roles before you map them to the BI platform to prevent specific users from logging on.

9.6.4 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your BI platform user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and BI platform users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- Update roles only: using this option will update only the links between the currently mapped roles that have been imported in the BI platform. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in the BI platform for new user aliases added to the ERP system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

9.6.4.1 To schedule user updates

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

1. Click the *User Update* tab.
2. Click *Schedule* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

   > **Tip**
   >
   > If you want to run an update immediately click *Update Now*.

   > **Tip**
   >
   > Use the *Update Roles Only* option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

   The *Recurrence* dialog box appears.
3. Select an option from the *Run Object* list and provide all the requested scheduling information.

   When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

   Table 49:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Recurrence pattern	Description
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule* after you have finished providing the scheduling information.
The date of the next scheduled role update is displayed in the *User Update* tab.

> **Note**
>
> You can always cancel the next scheduled update by clicking *Cancel Scheduled Updates* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

9.6.5 Using the PeopleSoft Security Bridge

The Security Bridge feature of the BI platform allows you to import PeopleSoft EPM security settings to the BI platform.

The Security Bridge operates in two modes:

- **Configuration mode**
  In configuration mode, the Security Bridge provides an interface that enables you to create a response file. This response file is what governs the behavior of the Security Bridge during execution mode.
- **Execution mode**
  Based on the parameters that you define in the response file, the Security Bridge imports the security settings of dimension tables in PeopleSoft EPM to universes in the BI platform.

9.6.5.1 Importing security settings

To import the security settings, you must do the following tasks in order:

- Define the objects that the Security Bridge will manage.
- Create a response file.
- Run the Security Bridge application.

For information about managing security after you import the settings, see Managing security settings [page 308].

9.6.5.1.1 Defining managed objects

Before you run the Security Bridge, it is important to determine the objects that are managed by the application. The Security Bridge manages one or more PeopleSoft roles, a BI platform group, and one or more universes.

- Managed PeopleSoft roles

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

These are roles in your PeopleSoft system. Members of these roles work with PeopleSoft data through PeopleSoft EPM. You must choose the roles that include the members for whom you want to provide/update access privileges to the managed universes in the BI platform.
The access rights that are defined for the members of these roles are based on their rights in PeopleSoft EPM; the Security Bridge imports these security settings to the BI platform.

- Managed BI platform group
  When you run the Security Bridge, the program creates a user in the BI platform for each member of a managed PeopleSoft role.
  The group in which the users are created is the managed BI platform group. Members of this group are the users whose access rights to the managed universes are maintained by the Security Bridge. Because the users are created in one group, you can configure the Security Bridge not to update the security settings for certain users simply by removing users from the managed BI platform group.
  Before you run the Security Bridge, you must choose a group in the BI platform to be the location where the users are created. If you specify a group that does not exist, the Security Bridge will create the group in the BI platform.
- Managed universes
  Managed universes are the universes to which the Security Bridge imports security settings from PeopleSoft EPM. From the universes that are stored in your BI platform system, you must choose which ones are to be managed by the Security Bridge. Members of managed PeopleSoft roles who are also members of the managed BI platform group cannot access any data through these universes that they cannot access from PeopleSoft EPM.

9.6.5.1.2 To create a response file

1. Go to the folder that you specified during the installation of the Security Bridge, and run the `crpsepmsecuritybridge.bat` (in Windows) and `crpsepmsecuritybridge.sh` (in Unix) file.

   > **Note**
   >
   > In Windows, by default, this location is `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`.

   The Security Bridge for PeopleSoft EPM dialog box appears.
2. Select *New* to create a response file, or select *Open* and click *Browse* to specify a response file that you want to modify. Select the language you want for the file.
3. Click *Next*.
4. Provide the locations of the *PeopleSoft EPM SDK* and the *BI Platform SDK*.

   > **Note**
   >
   > The PeopleSoft EPM SDK is typically located on the PeopleSoft server at `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.

   > **Note**
   >
   > The BI platform SDK is typically located at `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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:

   Table 50:

Field	Description
Database	The name of the PeopleSoft database.
Host	The name of the server that hosts the database.
Port number	The port number for accessing the server.
Class location	The location of the class files for the database driver.
User name	Your user name.
Password	Your password.

7. Click *Next*.

   The dialog box displays a list of all the classes that the Security Bridge will use to run. If necessary, you can add to or remove classes from the list.
8. Click *Next*.

   The dialog box prompts you for connection information for the BI platform.
9. Provide the appropriate information for the following fields:

   Table 51:

Field	Description
Server	The name of the server where the Central Management Server (CMS) is located.
User name	Your user name.
Password	Your password.
Authentication	Your authentication type.

10. Click *Next*.
11. Choose a BI platform group, and click *Next*.

    > **Note**
    >
    > The group that you specify in this field is where the Security Bridge creates users for the members of the managed PeopleSoft roles.

    > **Note**
    >
    > If you specify a group that does not already exist, it will be created by the Security Bridge.

    The dialog box displays a list of roles from your PeopleSoft system.
12. Select the *Imported* option for the roles that you want the Security Bridge to manage, and click *Next*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The Security Bridge creates a user in the managed BI platform group (which you specified in the previous step) for each member of the role(s) that you select.

The dialog box displays a list of universes in the BI platform.

13. Select the universe(s) to which you want the Security Bridge to import security settings, and click *Next*.
14. Specify a filename for the Security Bridge log file and a location where the log file will be saved. You can use the log file to determine whether or not the Security Bridge is successful in importing the security settings from PeopleSoft EPM.
15. Click *Next*.

    The dialog box displays a preview of the response file that the Security Bridge will use during execution mode.
16. Click *Save*, and choose a location where you want to save the response file.
17. Click *Next*.

    You have successfully created the response file for the Security Bridge.
18. Click *Exit*.

> **Note**
>
> The response file is a Java property file that you can also create and/or modify manually. For more details, see the "PeopleSoft response file" section.

9.6.5.2 Applying the security settings

To apply the security settings, run the `crpsepmsecuritybridge.bat` batch file (on Windows) or the `crpsempsecuritybridge.sh` file (on Unix), and use the response file that you created as an argument. For example, type **`crpsepmsecuritybridge.bat myresponsefile.properties`** on Windows, or **`crpsempsecuritybridge.sh myresponsefile.properties`** on Unix.

The Security Bridge application runs. It creates users in the BI platform for the members of the PeopleSoft roles that you specified in the response file and imports the security settings from PeopleSoft EPM to the appropriate universes.

9.6.5.2.1 Mapping considerations

During execution mode, the Security Bridge creates a user in the BI platform for each member of a managed PeopleSoft role.

The users are created to have only Enterprise authentication aliases, and the BI platform assigns random passwords to these users. As a result, the users cannot log on to the BI platform until the administrator manually reassigns new passwords or maps the role(s) to the BI platform through the PeopleSoft Security Plug-in to allow the users to log on by using their PeopleSoft credentials.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.6.5.3 Managing security settings

You can manage the security settings that you applied by modifying the objects that are managed by the Security Bridge.

9.6.5.3.1 Managed users

The Security Bridge manages users based on the following criteria:

- Whether or not the user is a member of a managed PeopleSoft role.
- Whether or not the user is a member of the managed BI platform group.

If you want to enable a user to access PeopleSoft data through universes in the BI platform, ensure that the user is a member of *both* a managed PeopleSoft role and the managed BI platform group.

- For members of managed PeopleSoft roles who do not have accounts in the BI platform, the Security Bridge creates accounts and assigns random passwords to them. The administrator must decide whether or not to reassign new passwords manually or map the roles to the BI platform through the PeopleSoft Security Plug-in to allow the users to log on to the BI platform.
- For members of managed PeopleSoft roles who are also members of the managed BI platform group, the Security Bridge updates the security settings that are applied to the users so that they have access to the appropriate data from the managed universes.

If a member of a managed PeopleSoft role has an existing account in the BI platform, but he or she is *not* a member of the managed BI platform group, then the Security Bridge *does not* update the security settings that are applied to the user. Typically, this situation occurs only when the administrator manually removes user accounts that have been created by the Security Bridge from the managed BI platform group.

> **Note**
>
> This is an effective method for managing security: by removing users from the managed BI platform group, you can configure their security settings to be different from the security settings that they have in PeopleSoft.

Conversely, if a member of the managed BI platform group is *not* a member of a managed PeopleSoft role, then the Security Bridge *does not* provide them with access to the managed universes. Typically, this situation occurs only when PeopleSoft administrators remove users who have been previously mapped to the BI platform by the Security Bridge from the managed PeopleSoft role(s).

> **Note**
>
> This is another method for managing security: by removing users from managed PeopleSoft roles, you can ensure that the users have no access to data from PeopleSoft.

9.6.5.3.2 Managed universes

The Security Bridge manages universes through restriction sets, which limit the data that managed users can access from the managed universes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Restriction sets are groups of restrictions (for example, restrictions to Query Controls, SQL Generation, and so on). The Security Bridge applies/updates Row Access and Object Access restrictions for the managed universes:

- It applies Row Access restrictions to dimension tables that are defined in PeopleSoft EPM. These restrictions are user-specific and can be configured to one of the following settings:
  - The user has access to all of the data.
  - The user has access to none of the data.
  - The user has access to data based on their row-level permissions in PeopleSoft, which are exposed through the Security Join Tables (SJT) that are defined in PeopleSoft EPM.
- It applies Object Access restrictions to measure objects based on the fields that are accessed by the measure objects.
  If a measure object accesses fields that are defined as metrics in PeopleSoft, then access to the measure object is allowed/disallowed depending on whether or not the user can access the referenced metrics in PeopleSoft. If a user cannot access any of the metrics, then access to the measure object is denied. If the user can access all of the metrics, then access to the measure object is granted.

As an administrator, you can also limit the data that users can access from your PeopleSoft system by limiting the number of universes that are managed by the Security Bridge.

9.6.5.4 PeopleSoft response file

The Security Bridge feature of the BI platform operates based on the settings that you specify in a response file.

Typically, you generate the response file by using the interface that is provided by the Security Bridge in configuration mode. However, because the file is a Java property file, you can also create or modify it manually.

This appendix provides information about the parameters that you need to include in the response file if you choose to generate it manually.

> **Note**
>
> When you create the file, you must respect the Java property file escaping requirement (for example, ':' is escaped as '\:').

9.6.5.4.1 Response file parameters

The following table describes the parameters that are included in the response file:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 52:

Parameter	Description
classpath	The class path for loading the necessary .jar files. Multiple class paths must be separated by a ';' on both Windows and UNIX. The class paths that are needed are for the `com.peoplesoft.epm.pf.jar` and the JDBC driver .jar files.
db.driver.name	The JDBC driver name that is used to connect to the PeopleSoft database (for example, `com.microsoft.jdbc.sqlserver.SQLServerDriver`).
db.connect.str	The JDBC connection string that is used to connect to the PeopleSoft database (for example, `jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO`)
db.user.name	The user name for logging on to the PeopleSoft database.
db.password	The password for logging on to the PeopleSoft database.
db.password.encrypted	The value for this parameter determines whether the password parameter in the response file is encrypted or not. The value can be set to either True or False. (If no value is specified, the value becomes False by default.)
enterprise.cms.name	The CMS in which the universes are located.
enterprise.user.name	The user name for logging on to the CMS.
enterprise.password	The password for logging on to the CMS.
enterprise.password.encrypted	The value for this parameter determines whether the password parameter in the response file is encrypted or not. The value can be set to either True or False. (If no value is specified, the value becomes False by default.)
enterprise.authMethod	The authentication method for logging on to the CMS.
enterprise.role	The managed BI platform group. For more information, see Defining managed objects [page 304].
enterprise.license	Controls the license type when importing users from PeopleSoft. "0" sets the named user license, "1" sets the concurrent user license.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description
peoplesoft.role.n	The list of managed PeopleSoft roles. For more information, see Defining managed objects [page 304]. **<n>** is an integer, and each entry occupies a property with the peoplesoft.role prefix. **Note** **<n>** is 1 based. You can use '*' to denote all available PeopleSoft roles, given that n is 1, and it is the only property that has peoplesoft.role as the prefix in the response file.
mapped.universe.n	The list of universes that you want the Security Bridge to update. For more information, see Defining managed objects [page 304]. **<n>** is an integer, and each entry occupies a property with the mapped.universe prefix. **Note** **<n>** is 1 based. You can use '*' to denote all available universes, given that n is 1, and it is the only property that has mapped.universe as the prefix in the response file.
log4j.appender.file.File	The log file that is written by the Security Bridge.
log4j.*	Default log4j properties that are required for log4j to function properly: log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description
peoplesoft classpath	The class path to the PeopleSoft EPM API .jar files. This parameter is optional.
enterprise.classpath	The class path to the BI platform SDK .jar files. This parameter is optional.
db.driver.type	The PeopleSoft database type. This parameter can have one of the following values: Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Custom Custom may be used to specify databases other than the recognized types or versions. This parameter is optional.
sql.db.class.location sql.db.host sql.db.port sql.db.database	The location of the SQL Server JDB driver .jar files, the SQL Server host machine, the SQL Server port, and the SQL Server database name. These parameter can be used only if the db.driver.type is Microsoft SQL Server 2000. These parameters are optional.
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	The location of the Oracle JDBC driver .jar files, the Oracle database host machine, the Oracle database port, and the Oracle database SID. These parameters can be used only if the db.driver.type is Oracle Database 10.1. These parameters are optional.
db2.db.class.location db2.db.host db2.db.port db2.db.sid	The location of the DB2 JDBC driver .jar files, the DB2 database host machine, the DB2 database port, and the DB2 database SID. These parameters can be used only if the db.driver.type is DB2 UDB 8.2 Fixpack 7 These parameters are optional.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description
custom.db.class.location custom.db.drivername custom.db.connectStr	The location, name, and connection string of the custom JDBC driver. These parameters can be used only if the db.driver.type is Custom. These parameters are optional.

9.7 JD Edwards authentication

9.7.1 Overview

To use your JD Edwards data with the BI platform, you must provide the system with information about your JD Edwards deployment. This information is what allows the BI platform to authenticate users so that they can use their JD Edwards EnterpriseOne credentials to log on to the BI platform.

9.7.2 Enabling JD Edwards EnterpriseOne authentication

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

9.7.2.1 To enable JD Edwards authentication in the BI Platform

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Double-click *JD Edwards EnterpriseOne*.
   The *JD Edwards EnterpriseOne* page appears.
4. On the *Options* tab, select the *Enable JD Edwards EnterpriseOne Authentication* check box.
5. Make appropriate changes under *New Alias*, *Update Options*, and *New User Options* according to your BI platform deployment. Click *Update* to save your changes before proceeding to the *Systems* tab.
6. Click the *Servers* tab.
7. Copy `jdeutil.jar`, `kernel.jar`, and `log4j.jar` from the JD Edwards installation to these locations (on Windows): **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` and **<INSTALLDIR>**`\Tomcat\lib\`.
8. Restart Tomcat and the Server Intelligence Agent.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9. In the *JD Edwards EnterpriseOne System User* area, type a database User name and Password for the BI platform to use to log on to your JD Edwards EnterpriseOne database.
10. In the *JD Edwards EnterpriseOne Domain* area, enter the name, host, and port used to connect to your JD Edwards EnterpriseOne environment, enter a name for the environment and click *Add*.
11. Click *Update* to save your changes.

9.7.3 Mapping JD Edwards EnterpriseOne roles to the BI Platform

The BI platform automatically creates a group for each JD Edwards EnterpriseOne role that you map. As well, the system creates aliases to represent the members of the mapped JD Edwards EnterpriseOne roles.

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in the BI platform.

Doing so reduces the number of accounts that are created for the same user in the BI platform.

For example, if you run a JD Edwards EnterpriseOne test environment and production environment, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in the BI platform.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

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

9.7.3.1 To map a JD Edwards EnterpriseOne role

1. Log on as an administrator to the Central Management Console.
2. From the *Manage* area, click *Authentication*.
3. Double-click *JD Edwards EnterpriseOne*.
4. In the *New Alias Options* area, select one of the following options:
   - *Assign each added alias to an account with the same name*
     Select this option if you run multiple JD Edwards EnterpriseOne Enterprise systems with users who have accounts on more than one system (and no two users have the same user name for different systems).
   - *Create a new account for every added alias*
     Select this option if you run only one JD Edwards EnterpriseOne, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. In the *Update Options* area, select one of the following options:
   - *New aliases will be added and new users will be created*
     Select this option to create a new alias for every user that is mapped to the BI platform. New accounts are added for users without BI platform accounts or for all users if you selected the Create a new account for every added alias option.
   - *No new aliases will be added and new users will not be created*
     Select this option if the role that you want to map contains many users, but only a few of them will use the BI platform. The system does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to the BI platform for the first time. This is the default option.
6. In the *New User Options* area specify how new users are created.
   Select one of the following options:
   - *New users are created as named users.*
     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.
   - *New users are created as concurrent users.*
     New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the BI platform, a 100 user concurrent license could support 250, 500, or 700 users.

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

9.7.3.2 Remapping consideration

If you add users to a role that has already been mapped to the BI platform, you need to remap the role to add the users to the BI platform. When you remap the role, the option to map users as either named users or concurrent users affects only the new users that you added to the role.

For example, you first map a role to the BI platform with the "New users are created as *named* users" option selected. Later, you add users to the same role and remap the role with the "New users are created as *concurrent* users" option selected.

In this situation, only the new users in the role are mapped to the BI platform as concurrent users; the users that were already mapped remain named users. The same condition applies if you first map users as concurrent users, and then you change the settings to remap new users as named users.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.7.3.3 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 *JD Edwards EnterpriseOne*.
4. In the *Roles* area, select the role that you want to remove, and click <.
5. Click *Update*.

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

   > **Note**
   >
   > You can also delete individual accounts or remove users from roles before you map them to the BI platform to prevent specific users from logging on.

9.7.4 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your BI platform user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and BI platform users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- Update roles only: using this option will update only the links between the currently mapped roles that have been imported in the BI platform. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in the BI platform for new user aliases added to the ERP system.

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

9.7.4.1 To schedule user updates

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

1. Click the *User Update* tab.
2. Click *Schedule* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

   > **Tip**
   >
   > If you want to run an update immediately click *Update Now*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Tip**
>
> Use the *Update Roles Only* option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

The *Recurrence* dialog box appears.

3. Select an option from the *Run Object* list and provide all the requested scheduling information.

   When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

   Table 53:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule* after you have finished providing the scheduling information.
   The date of the next scheduled role update is displayed in the *User Update* tab.

> **Note**
>
> You can always cancel the next scheduled update by clicking *Cancel Scheduled Updates* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.8 Siebel authentication

9.8.1 Enabling Siebel authentication

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

9.8.1.1 To enable Siebel authentication in the BI Platform

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

9.8.2 Mapping roles to the BI platform

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

You can create a user account for each alias that is created.

However, if you run multiple systems, and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in the BI platform.

Doing so reduces the number of accounts that are created for the same user in the program.

For example, if you run a Siebel eBusiness test environment and production environment, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in the BI platform.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

9.8.2.1 To map a Siebel eBusiness role to the BI Platform

1. Log on as an administrator to the Central Management Console.
2. Click *Authentication*.
3. Double-click *Siebel*.
4. Select the check box *Enable Siebel Authentication*.
5. In the *New Alias Options* area, select one of the following options:
   - *Assign each added alias to an account with the same name*
     Select this option if you run multiple Siebel eBusiness systems with users who have accounts on more than one system (and no two users have the same user name for different systems).
   - *Create a new account for every added alias*
     Select this option if you run only one Siebel eBusiness, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.
6. In the *Alias Update Options* area, select one of the following options:
   - *Create new aliases when the Alias Update occurs*
     Select this option to create a new alias for every user that is mapped to the BI platform. New accounts are added for users without BI platform accounts or for all users if you selected the Create a new account for every added alias option.
   - *Create new aliases only when the user logs on*
     Select this option if the role that you want to map contains many users, but only a few of them will use the BI platform. The program does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to the BI platform for the first time. This is the default option.
7. In the *New User Options* area specify how new users are created.
   If your BI platform license is based on users roles, select one of the following options:

   Select one of the following options:
   - *New users are created as named users*
     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.
   - *New users are created as concurrent users*
     New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the BI platform, a 100 user concurrent license could support 250, 500, or 700 users.
8. Click the *Roles* tab.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

> **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*.

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

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

9.8.2.2 Remapping consideration

To enforce group and user synchronization between the BI platform 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 the BI platform with the "New users are created as *named* users" option selected. Later, you add users to the same role and remap the role with the "New users are created as *concurrent* users" option selected.

In this situation, only the new users in the role are mapped to the BI platform as concurrent users; the users that were already mapped remain named users. The same condition applies if you first map users as concurrent users, and then you change the settings to remap new users as named users.

9.8.2.3 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*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. On the *Domains* tab select the Siebel domain that corresponds to the role or roles you want to unmap.
5. In the *Roles* tab select the role that you want to remove, and click <.
6. Click *Update*.

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

> **Note**
>
> You can also delete individual accounts or remove users from roles before you map them to the BI platform to prevent specific users from logging on.

9.8.3 Scheduling user updates

To ensure changes to your user data for your ERP system are reflected in your BI platform user data, you can schedule regular user updates. These updates will automatically synchronize your ERP and BI platform users according to the mapping settings you have configured in the Central Management Console (CMC).

There are two options for running and scheduling updates for imported roles:

- Update roles only: using this option will update only the links between the currently mapped roles that have been imported in the BI platform. Use this option if you expect to run frequent updates, and you are concerned about system resource usage. No new user accounts will be created if you only update roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in the BI platform for new user aliases added to the ERP system.

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

9.8.3.1 To schedule user updates

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

1. Click the *User Update* tab.
2. Click *Schedule* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

> **Tip**
>
> If you want to run an update immediately click *Update Now*.

> **Tip**
>
> Use the *Update Roles Only* option if you would like frequent updates and are concerned about system resources. It takes the system longer to update both roles and aliases.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The *Recurrence* dialog box appears.

3. Select an option from the *Run Object* list and provide all the requested scheduling information.

   When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

   Table 54:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule* after you have finished providing the scheduling information.
   The date of the next scheduled role update is displayed in the *User Update* tab.

> **Note**
>
> You can always cancel the next scheduled update by clicking *Cancel Scheduled Updates* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

9.9 Oracle EBS authentication

9.9.1 Enabling Oracle EBS authentication

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.9.1.1 To enable Oracle E-Business Suite authentication

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

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

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

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

Related Information

To map Oracle E-Business Suite roles [page 324]

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

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

You can create a user account for each alias that is created. However, if you run multiple systems and your users have accounts in more than one of the systems, then you can assign each user to an alias with the same name before you create the accounts in the BI platform.

Doing so reduces the number of accounts that are created for the same user in the system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

For example, if you run a EBS test environment and production environment, and 30 of your users have access to both systems, then only 30 accounts are created for those users. If you choose not to assign each user to an alias with the same name, then 60 accounts are created for the 30 users in the BI platform.

However, if you run multiple systems, and user names overlap, then you must create a new member account for each alias that is created.

For example, if you run your test environment with a user account for Russell Aquino (user name "raquino"), and you run the production environment with a user account for Raoul Aquino (user name "raquino"), then you need to create a separate account for each user's alias. Otherwise, the two users are added to the same BI platform account; they will be able to log on to the system with their own Oracle EBS credentials and have access to data from both EBS environments.

9.9.2.1 To map Oracle E-Business Suite roles

1. Log on as an administrator to the Central Management Console.
2. From the Manage area, click *Authentication*.
3. Click *Oracle EBS*.
   The *Oracle EBS* page displays the *Options* tab.
4. In the *New Alias Options* area, select one of the following options:
   - *Assign each added Oracle EBS alias to an account with the same name*
     Select this option if you run multiple Oracle E-Business Suite systems with users who have accounts on more than one system (and if no two users have the same user name for different systems).
   - *Create a new account for every added Oracle EBS alias*
     Select this option if you run only one Oracle E-Business Suite, if the majority of your users have accounts on only one of your systems, or if the user names overlap for different users on two or more of your systems.
5. In the *Update Options* area, select one of the following options:
   - *Create new aliases when the Alias Update occurs*
     Select this option to create a new alias for every user that is mapped to the BI platform. New accounts are added for users without BI platform accounts or for all users if you selected the *Create a new account for every added Oracle EBS alias* option.
   - *Create new aliases only when the user logs on*
     Select this option if the role that you want to map contains many users, but only a few of them will use the BI platform. The platform does not automatically create aliases and accounts for the users. Instead, it creates aliases (and accounts, if required) only for users when they log on to the BI platform for the first time. This is the default option.
6. In *New User Options* specify how new users are created, and then click *Update*.

   Select one of the following options:
   - *New users are created as named users.*
     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option.
   - *New users are created as concurrent users.*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to the BI platform at the same time. This type of licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access the platform, a 100 user concurrent license could support 250, 500, or 700 users.

The roles that you selected now appear as groups in the BI platform.

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

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

9.9.2.1.1 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 the BI platform. This will ensure that updated Oracle EBS role information is accurately reflected in the BI platform.

There are two options for running and scheduling updates for Oracle EBS roles:

- Update roles only: using this option will only update the links between the currently mapped roles that have been imported in the BI platform. It is recommended that you use this option if you expect to run frequent updates, and you have concerns over system resource usage. No new user accounts will be created if you only update Oracle EBS roles.
- Update roles and aliases: this option not only updates links between roles but will also create new user accounts in the BI platform for user aliases added to roles in the Oracle EBS system.

> **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.

9.9.2.1.2 To schedule updates for Oracle EBS roles

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

1. Click the *User Update* tab.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Click *Schedule* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

> **Tip**
>
> If you want to immediately run an update click *Update Now*.

> **Tip**
>
> Use the *Update Roles Only* option if you would like frequent updates and have concerns about system resources. It takes the system longer to update both roles and aliases.

The *Recurrence* dialog box appears.

3. Select an option from the *Run Object* pull-down list and provide all the requested scheduling information in the fields provided.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Table 55:

Recurrence pattern	Description
Hourly	The update will run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will run every day or every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will run every week. It can run once a week or several times a week. You can specify on which days and at what time it will run, as well as a start and end date.
Monthly	The update will run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as a start and end date.
Calendar	The update will run on the dates specified in a calendar that has previously been created.

4. Click *Schedule* after you have finished providing the scheduling information.
The date of the next scheduled role update is displayed in the *User Update* tab.

> **Note**
>
> You can always cancel the next scheduled update by clicking *Cancel Scheduled Updates* in either the *Update Roles Only* or *Update Roles and Aliases* sections.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.9.3 Unmapping roles

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

9.9.3.1 To unmap a role

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

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

   > **Note**
   >
   > You can also delete individual accounts or remove users from roles before you map them to the BI platform to prevent specific users from logging on.

9.9.4 Customizing rights for mapped Oracle EBS groups and users

When you map roles to the BI platform, you can set rights or grant permissions for the groups and users that are created.

9.9.4.1 To assign administration rights

To allow users to maintain the BI platform, you must make them members of the default Administrators group. Members of this group receive full control over all aspects of the system, including 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 and Groups*.
3. In the *Name* column, right-click *Administrators* and click *Add Members to Group*.

   The Available Users or Groups page appears.
4. From the *User List* or *Group List* area, select the mapped role to which you want to assign administrative rights.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. Click > to make the role a subgroup of the Administrators group, and click *OK*.

Members of the role now have administration rights in the BI platform.

> **Note**
>
> You can also create a role within Oracle EBS, add the appropriate users to the role, map the role to the BI platform, and make the mapped role a subgroup of the default Administrators group to grant members of the role administrative rights.

9.9.4.2 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 the BI platform.

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 or 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 and Assign Security*.

   The Assign Security page appears.
8. In the *Available Access Levels* 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, select a group, and click *Remove*.

9.9.5 Configuring Single Sign-on (SSO) for SAP Crystal Reports and Oracle EBS

By default, the BI platform will be configured to allow SAP Crystal Reports users to access Oracle EBS data using Single Sign-on (SSO).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9.9.5.1 To deactivate SSO for Oracle EBS and SAP Crystal Reports

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select *crdb_oraapps*.
5. Click *Remove*.
6. Click *Save & Close*.
7. Go to the *Servers* page in the CMC, and select *Crystal Reports Services*.
8. Click the *Restart server* button.

9.9.5.2 To reactivate SSO for Oracle EBS and SAP Crystal Reports

Follow the steps below to reactivate SSO for Oracle EBS and SAP Crystal Reports.

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Under *Use SSO context for database logon with the following drivers*, type **`crdb_oraapps`**.
5. Click *Add*.
6. Click *Save & Close*.
7. Go to the *Servers* page in the CMC, and select *Crystal Reports Services*.
8. Click the *Restart server* button.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10 Server Administration

10.1 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.

Table 56:

Navigation tree option	Description
Servers List	Displays a complete list of all servers in the deployment.
Server Groups List	Displays a flat list of all available server groups in the Details pane. Select this option if you want to configure a server group's settings or security.
Server Groups	Lists the server groups and the servers within each server group. When you select a server group, its servers and server groups are displayed in the Details pane in a hierarchical view.
Nodes	Displays a list of the nodes in your deployment. Nodes are configured in the CCM. You can select a node by clicking it to view or manage the servers on the node.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Navigation tree option	Description
Service Categories	Provides a list of the types of services that may be in your deployment. Service categories are divided into core BI platform services and services associated with specific SAP BusinessObjects components. Service categories include: • *Connectivity Services* • *Core Services* • *Crystal Reports Services* • *Data Federation Services* • *Promotion Management Services* • *Analysis Services* • *Web Intelligence Services* • *Dashboards Services* Select a service category in the navigation list to view or manage the servers in the category. **Note** A server may host services belonging to multiple service categories. Therefore a server can appear in several service categories.
Server Status	Displays the servers according to their current status. This is a valuable tool for checking to see which of your servers are running or stopped. If you are experiencing slow performance on the system, for example, you can use the *Server Status* list to quickly determine if any of your servers are in an abnormal state. Possible server states include the following: • *Stopped* • *Starting* • *Initializing* • *Running* • *Stopping* • *Started with Errors* • *Failed* • *Waiting for resources*

About the Details pane

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

Note

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 57:

Details pane column	Description
Server Name or *Name*	Displays the name of the server.
State	Displays the current status of the server. You can sort by server state using the *Server Status* list in the navigation tree. Possible server states include the following: • *Stopped* • *Starting* • *Initializing* • *Running* • *Stopping* • *Started with Errors* • *Failed* • *Waiting for resources*
Enabled	Displays whether the server is enabled or disabled.
Stale	If the server is marked as *Stale*, then it requires a restart. For example, if you change certain server settings in the server's *Properties* screen, you may need to restart the server before the changes will take effect.
Kind	Displays the type of server.
Host Name	Displays the Host Name for the server.
Health	Indicates the general health of the server. Possible server states include the following: • *Green* (healthy) • *Amber* (caution) • *Red* (danger) The health state of a server directly depends on the status of the server's watch. For example, the health state of the Central Management Server depends on the status of the `<NODENAME>.CentralManagementServer Watch`. You can access the details of watches on the *Monitoring* page in the CMC: on the *Watchlist* tab, select the watch and click *Edit*. You will see the *Caution Rule* and *Danger Rule* for the watch, which map to the amber and red health states, respectively.
PID	Displays the unique Process ID number for the server.
Description	Displays a description of the server. You can change this description in the server's *Properties* page.
Date Modified	Displays the date that the server was last modified, or when the server's state was changed. This column is very useful if you want to check the status of recently changed servers.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Managing server groups [page 347]
Using nodes [page 366]
Viewing the state of servers [page 333]
Starting, stopping, and restarting servers [page 335]
To change a server's properties [page 355]
Managing CMS system database connections [page 396]

10.2 Managing servers by using scripts on Windows

The `ccm.exe` executable lets you start, stop, restart, enable, and disable the servers in your Windows deployment through the command line.

Related Information

ccm.exe [page 814]

10.3 Managing servers on Unix

The `ccm.sh` executable lets you start, stop, restart, enable, and disable the servers in your Unix deployment through the command line.

Related Information

ccm.sh [page 807]

10.4 Viewing and changing a server's status

10.4.1 Viewing the state of servers

The status of a server is its current state of operation: a server can be running, starting, stopping, stopped, failed, initializing, started with errors, or waiting for resources. To respond to BI platform requests, a server must be

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

running and enabled. A server that is disabled is still running as a process; however, it is not accepting requests from the rest of the BI platform. A server that is stopped is no longer running as a process.

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

Related Information

To view a server's status [page 334]
To view the state of services [page 334]
Starting, stopping, and restarting servers [page 335]
Enabling and disabling servers [page 338]
Stopping a Central Management Server [page 337]
To automatically start a server [page 337]

10.4.1.1 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. The *State* column provides the status for each server in the list.
3. If you want to view a list of all of the servers that currently have a particular status, expand the *Server Status* option in the navigation tree and select the status you want.

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

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

Related Information

To view the state of services [page 334]

10.4.1.2 To view the state of services

If any service fails, the state of the host server is set to either *Started with Errors* (meaning that at least one service started successfully) or *Failed* (meaning that none of the services started successfully). You can view the

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

server states in the CMC and CCM. However, you can also view the status of individual services, on the server's *Properties* page in the CMC.

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

   The *Details* pane displays the service categories in your deployment.
2. To view a list of servers in a given Server Group, Node, or Service Category, in the navigation tree click the server group, node, or category.
   The *Details* pane displays the list of servers in your deployment.
3. Double-click a server to open its *Properties* page.

   The *Properties* page shows the properties for the server and the services it hosts. For failed services, error messages are also displayed.

Related Information

Viewing the state of servers [page 333]

10.4.2 Starting, stopping, and restarting servers

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

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

Table 58:

Action	Description
Stopping a server	You may need to stop BI platform servers before you can modify certain properties and settings.
Starting a server	If you stopped a server to configure it, you must restart the server before your changes will take effect and before the server can resume processing requests.
Restarting a server	Restarting a server is a shortcut to stopping a server completely and then starting it again. If you need to restart a server after changing a server setting, you will be prompted by the CMC.
Starting a server automatically	You can set servers to start automatically when the Server Intelligence Agent starts.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Action	Description
Force Termination	Stops a server immediately (whereas when you stop a server, it will stop when it has completed its current processing activities). Forcibly terminate a server only when stopping the server has failed and you need to stop the server immediately.

Tip

When you stop (or restart) a server, you terminate the server's process, thereby stopping the server completely. Before you stop a server, it is recommended that you

- Disable the server so it can finish processing any jobs it has in progress, and
- Ensure that there are no auditing events remaining in the queue. To view the number of auditing events remaining in the queue, navigate to the server's *Metrics* screen and view the *Current Number of Auditing Events in the Queue* metric.

Related Information

Enabling and disabling servers [page 338]

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

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

   The *Details* pane displays the service categories in your deployment.
2. To view a list of servers in a particular Server Group, Node, or Service Category, select the group, node, or category on the navigation pane.
   The *Details* pane displays a list of servers.
3. If you want to view a list of all of the servers that currently have a particular status, expand the *Server Status* option in the navigation tree and select the status you want.

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

   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*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Viewing the state of servers [page 333]

10.4.2.2 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.

10.4.2.3 To automatically start a server

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

1. Go to the *Servers* management area of the CMC.
2. Double-click the server you want to automatically start.
   The *Properties* screen appears.
3. Under *Common Settings*, select the *Automatically start this server when the Server Intelligence Agent starts* check box, and click *Save* or *Save & Close*.

> **Note**
>
> If the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster, you must use the CCM to restart the system. After using the CCM to stop the SIA, right-click the SIA and select *Properties*. On the *Startup* tab, click *Properties* to open the Server Properties page for the CMS. Select *Auto-Start*, then click *OK* to close the Server Properties page, and then click *OK* again. Restart the SIA. The *Autostart* option is available only when the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster.

10.4.3 Stopping a Central Management Server

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

However, if your BI platform deployment has a single CMS, shutting it down will make the BI platform unavailable to your users and will interrupt the processing of reports and programs. To avoid this problem, the Server

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Intelligence Agent for each node ensures that at least one CMS is running at all times. You can still stop a CMS by stopping its SIA, but before stopping the SIA, you should disable the processing servers via the CMC so that they can finish any jobs in progress before the BI platform shuts down, because all other servers on the node will also shut down.

> **Note**
>
> You may encounter situations where the CMS has been stopped and you need to restart the system from the CCM. For example, if you shut down each CMS on a node and the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster when the SIA starts, you must use the CCM to restart the system. In the CCM, right-click the SIA and choose *Properties*. On the *Startup* tab, click *Properties* to open the Server Properties page for the CMS. Select *Auto-Start*, then click *OK* to close the Server Properties page, and then click *OK* again. Restart the SIA. The *Autostart* option is available only when the *Automatically start this server when the Server Intelligence Agent starts* check box is cleared for each CMS in the cluster.

If you want to configure your system so that you can start and stop the Central Management Server in the cluster without starting and stopping other servers, put the CMS on a separate node. Create a new node and clone the CMS to the node. With the CMS on its own node, you can easily shut down the node without affecting other servers.

Related Information

Using nodes [page 366]
Cloning servers [page 340]
Clustering Central Management Servers [page 342]

10.4.4 Enabling and disabling servers

When you disable a BI platform server, you prevent it from receiving and responding to new BI platform requests, but you do not actually stop the server process. This is useful when you want to allow a server to finish processing all of its current requests before you stop it completely.

For example, you may want to stop a Job Server before rebooting the machine it is running on. However, you want to allow the server to fulfill any outstanding report requests that are in its queue. First, you disable the Job Server so it cannot accept any additional requests. Next, go to the Central Management Console to monitor when the server completes the jobs it has in progress. (From the *Servers* management area, right-click the server and select *Metrics*.) Then, once it has finished processing current requests, you can safely stop the server.

> **Note**
>
> The CMS must be running in order for you to enable and/or disable other servers.

> **Note**
>
> A CMS cannot be enabled or disabled.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.4.4.1 To enable and disable servers with the CMC

1. Go to the *Servers* management area of the CMC.
2. Right-click the server whose status you want to change, and depending on the action you need to perform click *Enable Server* or *Disable Server*.

10.4.4.2 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 the BI platform.
3. In the *Manage Servers* dialog box, select the server that you want to enable or disable.
4. Click *Enable* or *Disable*.
5. Click *Close* to return to the CCM.

10.5 Adding, cloning, or deleting servers

10.5.1 Adding, cloning, and deleting servers

If you want to add new hardware to the BI platform by installing server components on new, additional machines, run the BI platform installation program on those machines. The setup program allows you to perform a Custom installation. During the Custom installation, specify the CMS from your existing deployment, and select the components that you want to install on the local machine. For details on custom installation options, see the *SAP BI platform Installation Guide*.

10.5.1.1 Adding a server

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

1. Go to the *Servers* management area of the CMC.
2. On the *Manage* menu, click *New* > *New Server*.
   The *Create New Server* dialog box appears.
3. Choose the *Service Category*.
4. Choose the type of service that you need from the *Select Service* list, then click *Next*.
5. To add an additional service to the server, select the service in the *Available Additional Services* list and click *>*.

> **Note**
>
> Additional services are not available for all server types.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. After adding the additional services you want, click *Next*.
7. If your BI platform architecture is composed of multiple nodes, choose the node where you want to add the new server from the *Node* list.
8. Type a name for the server in the *Server Name* box.

   Each server on the system must have a unique name. The default naming convention is **<NODENAME>.<servertype>** (a number is appended if there is more than one server of the same type on the same host machine).
9. To include a description for the server, type it into the *Description* box.
10. If you are adding a new Central Management Server, specify a port number in the *Name Server Port* field.
11. Click *Create*.
    The new server appears in the list of servers in the *Servers* area of the CMC, but it is neither started nor enabled.
12. Use the CMC to start and enable the new server when you want it to begin responding to BI platform requests.

Related Information

Servers, services, nodes, and hosts [page 25]
Configuring server settings [page 354]
Configuring port numbers [page 363]
Viewing the state of servers [page 333]

10.5.1.2 Cloning servers

If you want to add a new server instance to your deployment, you can clone an existing server. The cloned server retains the configuration settings of the original server. 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 BI platform (and any updates, if applicable).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> You can clone servers from any machine. However, you can only clone servers to machines where the required binaries for the server are installed.

> **Note**
>
> When you clone a server, it does not necessarily mean that the new server will use the same OS credentials. The user account is controlled by the Server Intelligence Agent that the server is running under.

10.5.1.2.1 Using placeholders for server settings

Placeholders are node-level variables that are used by the servers that are running on the node. Placeholders are listed on a dedicated page in the Central Management Console (CMC). When you double-click any server listed under *Servers* in the CMC, a link is provided on the left-hand navigation pane for "Placeholders". The *Placeholders* page lists all the available placeholder names and their associated values for the selected server. Placeholders contain read-only values and the placeholder names begin and end with the percentage character `%`.

> **Note**
>
> You can always overwrite a placeholder setting with a specific string in the CMC Server *Properties* page.

> **Example**
>
> Placeholders are useful when cloning servers. For example, multi-drive machine A has the BI platform installed on `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. So the `%DefaultAuditingDir%` placeholder will be `D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.
>
> On another machine, machine B, there is only one disc drive (no drive D) and the BI platform is installed on `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. In this case the `%DefaultAuditingDir%` placeholder will be `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.
>
> To clone the Event Server from machine A to machine B, if placeholders are used for the Auditing Temporary Directory, the placeholders will resolve themselves and the Event Server will work properly. If no placeholders are used, the Event Server will fail unless you manually overwrite the Auditing Temporary Directory setting.

10.5.1.2.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

10.5.1.3 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*.

10.6 Clustering Central Management Servers

10.6.1 Clustering Central Management Servers

If you have a large or mission-critical implementation of SAP BusinessObjects Business Intelligence platform, you will probably want to run several CMS machines together in a cluster. A cluster consists of two or more CMS servers working together against a common CMS system database. If a machine that is running one CMS fails, a machine with another CMS will continue to service BI platform requests. This "high availability" support helps to ensure that BI platform users can still access information when there is an equipment failure.

This section shows how to add a new CMS cluster member to a production system that is already up and running. When you add a new CMS to an existing cluster, you instruct the new CMS to connect to the existing CMS system database and to share the processing workload with any existing CMS machines. For information about your current CMS, go to the *Servers* management area of the CMC.

Before clustering CMS machines, you must make sure that each CMS is installed on a system that meets the detailed requirements (including version levels and patch levels) for operating system, database server, database access method, database driver, and database client outlined in the Product Availability Matrix.

In addition, you must meet the following clustering requirements:

- For best performance, the database server that you choose to host the system database must be able to process small queries very quickly. The CMS communicates frequently with the system database and sends it many small queries. If the database server is unable to process these requests in a timely manner, BI platform performance will be greatly affected.
- For best performance, run each CMS cluster member on a machine that has the same amount of memory and the same type of CPU.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Configure each machine similarly:
  - Install the same operating system, including the same version of operating system service packs and patches.
  - Install the same version of the BI platform (including patches, if applicable).
  - Ensure that each CMS connects to the CMS system database in the same manner: whether you use native or ODBC drivers. Make sure that the drivers are the same on each machine, and are a supported version.
  - Ensure that each CMS uses the same database client to connect to its system database and that it is a supported version.
  - Check that each CMS uses the same database user account and password to connect to the CMS system database. This account must have create, delete, and update rights on the system database.
  - Ensure that the nodes on which each CMS is located are running under the same operating system account. (On Windows, the default is the "LocalSystem" account.)
  - Verify that the current date and time are set correctly on each CMS machine (including settings for daylight savings time).
  - Ensure that all machines in a cluster (including the machines that host the CMS) are set to the same system time. For best results, synchronize the machines to a time server (such as `time.nist.gov`) or use a central monitoring solution.
  - Ensure that the same WAR files are installed on all web application servers in the cluster. For more information on WAR file deployment, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*.
- Ensure that each CMS in a cluster is on the same Local Area Network.
- Out-of-Band threads (-oobthreads) are used by clustering pings and clustering notifications. Since both operations are quick (notifications are asynchronous), the BI platform no longer requires multiple oobthreads and only one -oobthread is created.
  If your cluster has more than eight CMS cluster members, ensure that the command line for each CMS includes the `-oobthreads` **`<numCMS>`** option, where **`<numCMS>`** is the number of CMS servers in the cluster. This option ensures that the cluster can handle heavy loads. For information about configuring server command lines, see the server command lines appendix in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
- 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 machine host-name of the first CMS that you install.

Related Information

Changing the name of a CMS cluster [page 346]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.6.1.1 Adding a CMS to a cluster

There are several ways to add a new CMS cluster member. Follow the appropriate procedure:

- You can install a new node with a CMS on a new machine.
- If you already have a node with CMS binary files, then you can add a new CMS server from the CMC.
- If you already have a node with CMS binary files, you can also add a new CMS server by cloning an existing CMS server.

> **Note**
>
> Back up your current CMS system database, server configuration, and the contents of your Input and Output File Repositories before making any changes. If necessary, contact your database administrator.

Related Information

Adding a new node to a cluster [page 344]
Adding a server [page 339]
Cloning servers [page 340]
Overview of backup and restore [page 442]

10.6.1.2 Adding a new node to a cluster

When you add a node (a node is a collection of BI platform servers managed by a single Server Intelligence Agent), you are prompted to either create a new CMS or to cluster the node to an existing CMS.

If you want to cluster a node to an existing CMS, you can also use the installation setup program. Run the BI platform installation and setup program on the machine where you want to install the new CMS cluster member. The setup program allows you to perform a custom installation. During the custom installation, specify the existing CMS whose system you want to expand, and select the components that you want to install on the local machine. In this case, specify the name of the CMS that is running on your existing system, choose to install a new CMS on the local machine, and provide the setup program with the information it needs to connect to your existing CMS system database. When the setup program installs the new CMS on the local machine, it automatically adds the server to your existing cluster.

> **Note**
>
> Before you cluster a new node to an existing CMS, if the new node is a brand new server, ensure that the BI platform installation on that server is at the same patch level as the existing BI platform environment.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Using nodes [page 366]

10.6.1.3 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.

10.6.1.3.1 To define cluster properties for the BOE web application

1. Access the custom folder for the `BOE.war` file on the machine hosting the web applications:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 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 using a text editor.
3. Specify the CMS cluster properties.

   Use the `cms.clusters` property to specify all the clusters in the deployment. Cluster names must be preceded by `@` characters and separated by commas. For example, `cms.clusters=@samplecluster,@samplecluster2,@samplecluster3`. Use the `cms.clusters.<[cluster name]>` property to specify every CMS contained 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
   ```

   > **Note**
   >
   > The port number is separated from the CMS name with a colon; The port number is assumed to be 6400 unless it is specified.

4. Save the file under the following name:

   `PlatformServices.properties`
5. Restart your application server.

The new properties take affect 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 *SAP BusinessObjects Business Intelligence platform Web Application Deployment Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.6.1.4 Changing the name of a CMS cluster

This procedure allows you to change the name of a cluster that is already installed. After changing the name of the CMS cluster, the Server Intelligences Agent automatically reconfigures each SAP Business Objects server so that it registers with the CMS cluster, rather than with an individual CMS.

> **Note**
>
> For experienced administrators of the BI platform, note that you can no longer use the `-ns` option on the server command line to configure which CMS a server should register with. This is now handled automatically by the SIA.

10.6.1.4.1 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.

10.6.1.4.2 To change the cluster name on UNIX

Use the `cmsdbsetup.sh` script. For reference, see the “Unix scripts” topic in the Command Line Administration chapter in the *BI platform Administrator Guide*.

Related Information

Unix scripts [page 807]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.7 Managing server groups

Server groups can organize and help to manage BI platform servers on your system. You can select a particular server or server group per publication (not per user), and you can group servers by region or type.

Group servers by region to easily set up default processing settings, recurrent schedules, and scheduling destinations for users who work in a particular regional office. You can associate a report object (such as a Crystal report or a Web Intelligence document) with a single server group so the object is always processed by the same servers, and you can associate scheduled report objects with a particular server group to ensure that scheduled objects are sent to the correct printers, file servers, and so on. Server groups are especially useful when maintaining systems that span multiple locations and time zones.

Server groups are especially useful when maintaining systems that span multiple locations and time zones. For example, use server groups to customize your BI platform system for reports viewed in different locations and for different report types. When organizing servers by region, you can perform the following actions for server groups:

- Configure default processing settings
- Configure recurrent schedules
- Configure scheduling destinations for users who work in a particular regional office
- Associate a report object (such as a Crystal report or a Web Intelligence document) with a single server group so the object is always processed by the same servers
- Associate scheduled report objects with a particular server group to ensure that scheduled objects are sent to the correct printers, file servers, and so on

Group servers by type when configuring objects to be processed by servers that are optimized for those objects.

After creating server groups, configure objects to use specific server groups for scheduling or viewing and modifying reports. Use the navigation tree in the *Servers* management area of the CMC to view server groups. The *Server Groups List* option displays a list of server groups in the *Details* pane, and the *Server Groups* option allows you to view the servers in the group.

Example

Grouping processing servers by type

For example, processing servers need to communicate frequently with the database containing data for published reports. Placing processing servers close to the database server that they need to access improves system performance and minimizes network traffic. Therefore, for a number of reports that run against a DB2 database, you can create a group of processing servers that process reports only against the DB2 database server. To improve system performance when viewing reports, you can configure the reports to always use this processing server group for viewing.

10.7.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.7.1.1 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 Information

Viewing the state of servers [page 333]

10.7.2 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.

10.7.2.1 To add subgroups to a server group

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

10.7.2.2 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*.

10.7.3 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.

10.7.3.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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*.

10.7.4 Administrative access to servers and server groups for users

Granting administrative rights to users enables them to perform server and server group tasks, such as starting and stopping servers.

Depending on your system configuration and security concerns, you may limit server management to the BI platform administrator or you may need to provide administrative access to other people using those servers. Many organizations have a group of IT professionals dedicated to server management. If your server team needs to perform regular server maintenance tasks that require them to shut down and start up servers, you need to grant them administrative rights to the servers. You may also want to delegate BI platform server administration tasks to other people or want some groups in your organization to control their own server management.

> **Note**
>
> You can select a server or server group for a publication (not for a particular user). However, you can assign administrative rights to users or user groups for a particular server or server group.

10.7.4.1 Granting administrative access rights to a server or a server group

You can assign administrative rights to users or user groups for a particular server or server group.

> **Note**
>
> You can select a server or server group for a publication (not for a user).

1. Go to the *Servers* management area of the CMC.
2. Right-click the server or server group for which to grant administrative access rights and select *User Security*.
3. Click *Add Principals* to add users or groups for whom to give administrative rights to the server or server group.
4. In the *Add Principals* dialog box, select a user or group for whom to give administrative rights to the server or server group, and click >.
5. Click *Add and Assign Security*.
6. On the *Assign Security* screen, select security settings for the user or group, and click *OK*.

Related Information

How rights work in BI platform [page 112]

 © 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.7.4.2 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

Users must also have permission to add objects to at least one folder before they can save new reports back to the BI platform.

To ensure that users retain the ability to perform additional reporting tasks (such as copying, scheduling, printing, and so on), it's recommended that you first assign the appropriate access level and update your changes. Then, change the access level to Advanced, and add any of the required rights that are not already granted. For instance, if users already have View On Demand rights to a report object, you allow them to modify the report by changing the access level to Advanced and explicitly granting the additional Edit objects right.

When users view reports through the Advanced DHTML viewer and the RAS, the View access level is sufficient to display the report, but View On Demand is required to actually use the advanced search features. The extra Edit objects right is not required.

10.8 Configuring Adaptive Processing Servers for production systems

The installation program installs one Adaptive Processing Server (APS) per host system. Depending on the features that you've installed, this APS may host a large number of services, such as the Monitoring Service, Promotion Management Service, Multi-Dimensional Analysis Service (MDAS), Publishing Service, and others.

For production or test systems, the best practice is to create additional APSs, and configure the APSs to meet your business requirements.

You can create additional APSs in two ways:

- Run the System Configuration Wizard.
  The wizard helps you with basic configurations of your BI platform system, including configuring APSs according to predefined deployment templates. The APS configuration provided by the wizard is a good starting point; however, system sizing must still be performed.
  The wizard is available from the Central Management Console (CMC). For more information about the wizard, see Introduction to the System Configuration Wizard [page 78]. For more information about default deployment templates, see the *SAP BusinessObjects BI platform Deployment Templates* document, which is available from within the wizard, and also at http://help.sap.com/bobip41.
- Use the CMC to manually create and configure additional APSs. For details, see Adding, cloning, and deleting servers [page 339].

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Remember

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

10.9 Assessing your system's performance

10.9.1 Monitoring BI platform servers

The Monitoring application provides the ability to capture the runtime and historical metrics of BI platform servers, for reporting and notification. The application helps system administrators to identify if servers are functioning normally and if the response times are as expected.

Related Information

About Monitoring [page 607]

10.9.2 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.

10.9.2.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To change a server's properties [page 355]
About the Server Metrics Appendix [page 902]

10.9.3 Viewing system metrics

The *Settings* management area of the CMC displays system metrics that provide general information about your BI platform installation. The *Properties* section includes information about the product version and build. It also lists the data source, database name, and database user name of the CMS database. The *View global system metrics* section lists current account activity, along with statistics about current and processed jobs. The *Cluster* section lists the name of the CMS you are connected to, the name of the CMS cluster, and the names of other cluster members.

10.9.3.1 To view system metrics

1. Go to the *Settings* management area of the CMC.
2. Click an arrow to expand and view the settings in the *Properties*, *View Global System Metrics*, *Cluster*, or *Hot Backup* area.

10.9.4 Logging server activity

The BI platform allows you to log specific information about BI platform web activity.

- In addition, each of the BI platform servers is designed to log messages to your operating system's standard system log.
  - On Windows, the BI platform logs to the Event Log service. You can view the results with the Event Viewer (in the Application Log).
  - On UNIX, the BI platform logs to the syslog daemon as a User application. Each server prepends its name and PID to any messages that it logs.

Each server also logs assert messages to the logging directory of your product installation. The programmatic information logged to these files is typically useful only to SAP BusinessObjects support staff for advanced debugging purposes. The location of these log files depends upon your operating system:

- On Windows, the default logging directory is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\logging`.
- On UNIX, the default logging directory **<INSTALLDIR>**`/sap_bobj/logging` directory of your installation.

The important point to note is that these log files are cleaned up automatically, so there will never be more than approximately 1 MB of logged data per server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> To enable logging to function on UNIX machines that are hosting BI platform servers, you must set up and configure system logging so that all messages logged to the “user” facility of “info” level or higher are recorded. You must also configure `SYSLOGD` to accept remote logging.
>
> Setup procedures vary from system to system. Consult your operating system documentation for specific instructions.

10.10 Configuring server settings

This section includes technical information and procedures that show how you can modify settings for BI platform servers.

The majority of the settings discussed in this section allow you to integrate the BI platform more effectively with your current hardware, software, and network configurations. Consequently, the settings that you choose will depend largely upon your own requirements.

You can change server settings though the Central Management Console (CMC) in two ways.

- On the *Properties* screen for the server.
- On the *Edit Common Services* screen for the server.

It is important to note that not all changes occur immediately. If a setting cannot change immediately, the *Properties* and *Edit Common Services* screens display both the current setting (in red text) and the desired setting. When you return to the Servers management area, the server will be marked as Stale. When you restart the server, it will use the desired settings and the Stale flag is removed from the server.

> **Note**
>
> This section does not show how to configure your Web application server to deploy BI platform applications. This task is typically performed when you install the product. For details, see the *SAP BusinessObjects Business Intelligence platform Installation Guide*.

Related Information

Configuring port numbers [page 363]
To change a server's properties [page 355]
Recreating the CMS system database [page 400]
Selecting a new or existing CMS database [page 398]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.10.1 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.

10.10.2 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.

10.10.3 Working with configuration templates

Configuration templates allow you to easily configure multiple instances of servers. Configuration templates store a list of settings for each service type, which you can use to configure additional server instances. For example, if you have a dozen Web Intelligence Processing Servers that you want to configure identically, you only need to configure settings for one of them. You can then use the configured service to define the configuration template for Web Intelligence Processing Servers, and then apply the template to the other 11 service instances.

Each type of BI platform service has its own configuration template. For example, there is one configuration template for the Web Intelligence Processing service type, one for the Publishing service type, and so on. The configuration template is defined in the server properties in the Central Management Console (CMC).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

When you make a server use a configuration template, existing settings for the server are overwritten with the values from the template. If you later decide to stop using the template, the original settings are not restored. Subsequent changes to the configuration template no longer affect the server.

It is good practice to use configuration templates as follows:

1. Set the configuration template on one server.
2. Assuming you want the same configuration on all servers of the same type, check *Use Configuration Template* for all servers of the same type, including the one where you set the configuration template.
3. Later, if you want to change the configuration of all services of this type, view the properties of any one of the services, deselect the *Use Configuration Template* check box. Change the settings you want, then select *Set Configuration Template* for this server and click *Save*. All services of that type are updated. By not having a server that is always set as the configuration template, you ensure that you will not accidentally change configuration settings for all servers of that type.

Related Information

To set a configuration template [page 356]
To apply a configuration template to a server [page 357]

10.10.3.1 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 Information

To apply a configuration template to a server [page 357]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.10.3.2 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 Information

To set a configuration template [page 356]

10.10.3.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.11 Configuring server network settings

The networking settings for BI platform servers are managed through the CMC. These settings are divided into two categories: port settings and host identification.

Default settings

During installation, server host identifiers are set to *Auto assign*. Each server can however be assigned either a specific IP address or a hostname. The default CMS port number is 6400. The other BI platform servers dynamically bind to available ports. Port numbers are automatically managed by the BI platform, but you can use the CMC to specify port numbers.

10.11.1 Network environment options

The BI platform supports both Internet Protocol version 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. The BI platform does not provide a mechanism to designate a networking environment. You can use the CMC to bind to a specific IPv6 or IPv4 address for any of your BI platform servers.

10.11.1.1 Mixed IPv6/IPv4 environment

The IPv6/IPv4 networking environment enables the following:

- BI platform servers can service both IPv6 and IPv4 requests when running in mixed IPv6/IPv4 mode.
- Client components can interoperate with servers as 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.11.2 Server host identification options

Host identification options can be specified in the CMC for all BI platform servers. The following table summarizes the options available in the *Common Settings* area:

Option	Description
Auto assign	This is the default setting for all servers. When this check box is selected, the server automatically binds the server's request port onto the first network interface on the machine. **Note** It is good practice to select the *Auto assign* check box for the host name. However, in some cases, such as when the server is running on multi-homed machine, or when the server needs to inter-operate with a certain firewall configuration, you should consider using either a specific hostname or IP address. See the information about configuring a multihomed machine and working with firewalls in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
Hostname	Specifies the host name of the network interface that the server listens for requests on. For the CMS, this setting specifies the host name of the network interface that the CMS binds the name server port and the request port.
IP Address	Specifies the IP address of the network interface that the server listens for requests on. For the CMS, it specifies the address of the network interface that the CMS uses to bind the name server port to the request port. For all servers, separate fields are provided to specify IPv4 and/or IPv6 IP addresses.

Caution

If you select the *Auto assign* check box on a multi-homed machine, the CMS may automatically bind to the wrong network interface. To avoid this, make sure the network interfaces on the host machine are listed in the correct order (using the machine's operating system tools). You must specify the host name for the CMS in the CMC.

Note

If you are working with multi-homed machines or in some NAT firewall configurations, you may need to specify the host name using fully qualified domain names instead of host names.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To configure the system for firewalls [page 173]
Configuring a multi-homed machine [page 360]
To troubleshoot multiple network interfaces [page 362]

10.11.2.1 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
Auto assign	The server will bind to one of the available network interfaces.
Hostname	Enter the host name of the network interface on which server listens for requests.
IP Address	Enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface on which server listens for requests. **Note** To enable the server to operate as a dual IPv4/IPv6 node, enter a valid IP address in both fields.

5. Click *Save* or *Save & Close*.
   The changes are reflected in the command line displayed on the *Properties* tab.
6. Start and enable the server.

10.11.3 Configuring a multi-homed machine

A multi-homed machine is one that has multiple network addresses. You may accomplish this with multiple network interfaces, each with one or more IP addresses, or with a single network interface that has been assigned multiple IP addresses.

If you have multiple network interfaces, each with a single IP address, change the binding order so that the network interface at the top of the binding order is the one you want the BI platform servers to bind to. If your interface has multiple IP addresses, use the Host Identifiers option in the CMC to specify a network interface card for the BI platform server. It can be specified by host name or IP address. For more information about configuring the *Host Identifiers* setting, see “To troubleshoot multiple network interfaces”.

Tip

This section shows how to restrict all servers to the same network address, but it is possible to bind individual servers to different addresses. For instance, you might want to bind the File Repository Servers to a private address that is not routable from users' machines. Advanced configurations such as this require your DNS

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

configuration to route communications effectively between all the BI platform server components. In this example, the DNS must route communications from the other BI platform servers to the private address of the File Repository Servers.

Related Information

To troubleshoot multiple network interfaces [page 362]

10.11.3.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.11.3.2 Configuring the remaining servers to bind to a network address

The remaining BI platform servers select their ports dynamically by default. For information on disabling the Auto assign setting that dynamically propagates this information, see “To change the port a server uses for accepting requests ”.

Related Information

To change the port a server uses for accepting requests [page 365]

10.11.3.3 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 the BI platform to bind to a non-primary routable network interface. Perform these steps immediately after installing the BI platform on the local machine, before you install the BI platform on other machines.

1. Open the CCM and stop the SIA for the node on the machine that has multiple network interfaces.
2. Right-click the SIA and choose *Properties*.
3. In the *Properties* dialog box, click the *Configuration* tab.
4. To bind the SIA to a specific network interface, type the port number of the target network interface in the *Port* field.
5. Click *OK* and select the *Startup* tab.
6. From the *Local CMS Servers* list select the CMS and click *Properties.*
7. To bind the CMS to a specific network interface, type the port number of the target network interface in the *Port* field.
8. Click *OK* to apply the new settings.
9. Start the SIA and wait for the servers to start.
10. Launch the Central Management Console (CMC), and go to the *Servers* management area. Repeat steps 11-14 for each server.
11. Select the server, then choose *Stop Server* from the *Actions* menu.
12. Choose *Properties* from the *Manage* menu.
13. Under *Common Settings*, select one of the following options:
    - Hostname: enter the host name of the network interface to which the server will bind.
    - IP Address: enter in the fields provided either an IPv4 or an IPv6 IP address for the network interface to which the server will bind.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **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.

10.11.4 Configuring port numbers

During installation, the CMS is set up to use default port numbers. The default CMS port number is 6400. This port falls within the range of ports reserved by SAP BusinessObjects (6400 to 6410). Communication on these ports should not conflict with third-party applications.

When started and enabled, each of the other BI platform servers dynamically binds to an available port (higher than 1024), registers with this port on the CMS, and then listens for BI platform requests. If necessary, you can instruct each server component to listen on a specific port (rather than dynamically selecting any available port). For example, you will need to manually configure a request port for each BI platform server that must communicate across a firewall.

Port numbers can be specified on each server's Properties tab in the CMC. This table summarizes the options under the *Common Settings* area as they relate to port usage for specific server types:

Table 59:

Setting	CMS	Other Servers
Request Port	Specifies the port that the CMS uses for accepting all requests from other servers (except for Name Server requests). Uses the same network interface as the Name Server Port. When *Auto assign* is selected, the server automatically uses an OS-assigned port number.	Specifies the port on which the server listens for all requests. When *Auto assign* is selected, the server automatically uses a port number assigned by the OS.
Name Server Port	Specifies the BI platform port on which the CMS listens for name service requests. The default is 6400.	Not applicable.

10.11.4.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **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.

10.11.4.2 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 the port number in the *Port* field.
6. Click *OK* to apply the new settings.
7. Start the SIA and wait for the servers to start.

10.11.4.3 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, 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Select *3 - Modify node*, and press `Enter`.
4. Select the node that hosts the CMS that you want to modify, and press `Enter`.
5. Select *3 - Modify a local CMS*, and press `Enter`.
   A list of CMSs hosted on the node appears.
6. Select the CMS to modify, and press `Enter`.
7. Type the new port number for the CMS, and press `Enter`.
8. Specify whether you want the CMS to automatically start when the SIA starts, and press `Enter`.
9. Type the command-line arguments for the CMS or accept the current arguments, and press `Enter`.
10. Type `quit` to exit the script.
11. Start the SIA with the `ccm.sh` script, and wait for the servers to start.

10.11.4.4 To change the port a CMS uses for accepting requests

1. Go to the *Servers* management area of the CMC.
2. Select the CMS, then choose *Properties* from the *Manage* menu.
3. Under *Common Settings*, deselect the *Auto assign* check box for *Request Port*, then type the port number you want the server to listen on.
4. Click *Save* or *Save & Close*.
5. Restart the CMS.

The CMS binds to the new port, and starts listening for requests from other servers.

10.11.4.5 To change the port a server uses for accepting requests

> **Note**
>
> These steps cannot be used to change the request port for the Central Management Server (CMS). See “To change the port a CMS uses for accepting requests” instead.

1. Go to the *Servers* management area of the CMC.
2. Select the server, then choose *Stop Server* from the *Actions* menu.
3. 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 BI platform requests on the new port.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.12 Managing Nodes

10.12.1 Using nodes

A node is a group of BI platform servers that run on the same host and are managed by the same Server Intelligence Agent (SIA). All servers on a node run under the same user account. One machine can contain many nodes so you can run processes under different user accounts. One SIA manages and monitors all servers on a node, ensuring they operate properly.

> **Note**
>
> You must use an Administrator account with Enterprise authentication to perform all node management procedures securely. However, if SSL communication between servers is enabled, you must disable SSL before you can perform node management tasks.

> **Note**
>
> Ensure that all database drivers needed for any BI platform servers to connect to their datasources (for example, for the CMS to connect to the CMS database) are present, and that the correct environment has already been set up (for example, appropriate environment variables have been set).

Related Information

Configuring servers for SSL [page 156]
To prepare a Unix machine for SQL Anywhere [page 367]

10.12.1.1 Variables

Variable	Description
<INSTALLDIR>	The directory where SAP BusinessObjects Business Intelligence platform is installed. On Windows: `C:\Program Files (x86)\SAP BusinessObjects`
<SCRIPTDIR>	The directory where node management scripts are located. • On Windows: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Variable	Description
	• On Unix: **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM64>**/scripts
<PLATFORM32>	The name of your Unix operating system. Acceptable values are: • aix_rs6000 • linux_x86 • solaris_sparc • win32_x86
<PLATFORM64>	The name of your Unix operating system. Acceptable values are: • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • win64_x64

10.12.1.2 To prepare a Unix machine for SQL Anywhere

You must create an odbc.ini file and source it before you can use SQL Anywhere as an ODBC data source on a Unix machine.

> **Note**
>
> This procedure is unnecessary if you use the bundled SQL Anywhere installed with the BI platform.

1. Create odbc.ini in **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM64>**.
2. Enter the database source name (DSN), the database name and server name for SQL Anywhere, and the IP address and port number of the machine that hosts the SQL Anywhere database server.
3. Save odbc.ini.
4. Bring the SQL Anywhere environment into your current environment.

   For example, if you are using Bash as your command line shell, source the 64-bit version of sa_config.sh.
5. Define an environment variable named ODBCINI that points to where the odbc.ini file was created.

   Set up that environment variable so that child processes can see the ODBCINI environment variable.

> **Example**
>
> A sample odbc.ini file:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0

[SampleDatabase]
UID=Administrator
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

A sample `source` command:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

Related Information

Variables [page 366]

10.12.2 Adding a new node

The installation program creates a single node when you first install the BI platform.

You may need additional nodes if you want to run servers under different user accounts.

You can add a new node using the Central Configuration Manager (CCM), or using a node management script. If you use a firewall, ensure that the ports of your Server Intelligence Agent (SIA) and Central Management Server (CMS) are open.

> **Note**
>
> Use the CCM or node management script on the machine where you want to add a node. It is not possible to add a node on a remote machine.

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

Remember that all machines in the cluster must have the same version and patch level.

10.12.2.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Tip**
>
> During the installation, click *Expand*, and specify your existing Central Management Server.

If you want to create additional nodes, use the Central Configuration Manager or the `serverconfig.sh` script.

For more information on installation, see the *SAP BI platform Installation Guide*.

10.12.2.2 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 number for the existing CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key.
   - If your deployment is stopped, select *Start a new temporary CMS*, and click *Next*.
     If prompted, enter the host name and port number for the temporary CMS, the Administrator credentials, the data source name, the database credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > **Caution**
     >
     > Avoid using the deployment while the temporary CMS runs. Ensure that the existing and new CMS use different ports.
5. Review the confirmation page, and click *Finish*.
   The CCM creates a node. If any errors occur, review the log file.

You can now use the CCM to start the new node.

10.12.2.2.1 Adding a node on Windows using a script

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you add a node.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

You can use `AddNode.bat` to add a node on a Windows machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in these parameters, unless you enclose the text within quotation marks.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
  -siaport 6415
      -cms mycms:6400
      -username Administrator
      -password My^ Password
      -cmsport 7400
      -dbdriver mysqldatabasesubsystem
      -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
      -dbkey abc1234
      -noservers
      -createcms
```

Note

To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

Related Information

Variables [page 366]
Script parameters for adding, recreating, and deleting nodes [page 383]

10.12.2.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- *default servers*
  Creates only the servers installed on this machine. It does not include all possible servers.

6. Select a CMS.
   - If your deployment is running, select *existing*, and press Enter.
     If prompted, enter the host name and port number for the existing CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key.
   - If your deployment is stopped, select *temporary*, and press Enter.
     If prompted, enter the host name and port number for the temporary CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     Caution

     Avoid using the deployment while the temporary CMS runs. Ensure that the existing and new CMS use different ports.

7. Review the confirmation page, and press Enter.
   The CCM creates a node. If any errors occur, review the log file.

You can now run **<INSTALLDIR>**`/sap_bobj/ccm.sh -start` **<nodeName>** to start the new node.

10.12.2.3.1 Adding a node on Unix using a script

Caution

Back up the server configuration for the entire cluster before and after you add a node.

You can use `addnode.sh` to add a node on a Unix machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
  -createcms
```

Related Information

Variables [page 366]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Script parameters for adding, recreating, and deleting nodes [page 383]

10.12.3 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.

Related Information

Restoring your system [page 451]

10.12.3.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- If the node does not exist in the system database of the CMS, a new node with default servers is added. Default servers include all of the servers installed on the host.

4. Select a CMS.
   - If your CMS is running, select *Use existing running CMS*, and click *Next*.
     If prompted, enter the host name and port number for the existing CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key.
   - If your CMS is stopped, select *Start a new temporary CMS*, and click *Next*.
     If prompted, enter the host name for the temporary CMS, the Administrator credentials, the data source name, the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     Caution

     Avoid using the deployment while the temporary CMS runs.

5. Review the confirmation page, and click *Finish*.
   The CCM recreates the node, and adds information about the node to the local machine. If any errors occur, review the log file.

You can now use the CCM to start the recreated node.

10.12.3.1.1 Recreating a node on Windows using a script

You can use `AddNode.bat` to recreate a node on a Windows machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in these parameters, unless you enclose the text within quotation marks.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
  -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
  -adopt
```

Note

To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Variables [page 366]
Script parameters for adding, recreating, and deleting nodes [page 383]

10.12.3.2 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 number for the existing CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key.
   - If your deployment is stopped, select *temporary*, and press Enter.
     If prompted, enter the host name for the temporary CMS, the Administrator credentials, the database connection information and the credentials for the system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > **Caution**
     >
     > Avoid using the deployment while the temporary CMS runs.

7. Review the confirmation page, and press Enter.
   The CCM recreates the node, and adds information about the node to the local machine. If any errors occur, review the log file.

You can now run **<INSTALLDIR>**/sap_bobj/ccm.sh -start **<nodeName>** to start the recreated node.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.12.3.2.1 Recreating a node on Unix using a script

You can use `addnode.sh` to recreate a node on a Unix machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

Related Information

Variables [page 366]
Script parameters for adding, recreating, and deleting nodes [page 383]

10.12.4 Deleting a node

You can delete a stopped node using a running Central Configuration Manager (CCM), or using a node management script. Use the following guidelines:

- Deleting a node also permanently deletes the servers on the node.
- If your cluster has multiple machines, delete the nodes before you remove a machine from the cluster and uninstall the software from it. If you remove a machine from a cluster before deleting a node, or if the file system on a machine malfunctions, you must recreate the node on a different machine with the same servers, in the same cluster, and then delete the node.

Remember

You can delete a node only on the machine where the node is located.

Related Information

Recreating a node [page 372]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.12.4.1 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 host name, port, and Administrator credentials for the CMS.

The CCM deletes the node and all the servers on the node.

10.12.4.1.1 Deleting a node on Windows using a script

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you delete a node.

You can use `RemoveNode.bat` to delete a node on a Windows machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

> **Example**

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Related Information

Variables [page 366]
Script parameters for adding, recreating, and deleting nodes [page 383]

10.12.4.2 To delete a node on Unix

Before and after you delete a node, back up the server configuration for the entire cluster.

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`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Select the node you want to delete, and press `Enter`.
5. If prompted, enter the host name, port number, and Administrator credentials for the CMS.

The node and all the servers on the node are deleted.

10.12.4.2.1 Deleting a node on Unix using a script

Caution

Back up the server configuration for the entire cluster before and after you delete a node.

You can use `removenode.sh` to delete a node on a Unix machine. For more information, see the "Script parameters for adding, recreating, and deleting nodes" section.

Example

```
<SCRIPTDIR>\removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Related Information

Variables [page 366]
Script parameters for adding, recreating, and deleting nodes [page 383]

10.12.5 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Adding a new node [page 368]
Cloning servers [page 340]
Deleting a node [page 375]

10.12.5.1 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 Information

Adding a new node [page 368]
Cloning servers [page 340]
Deleting a node [page 375]

10.12.5.2 To rename a node on Unix

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you rename a node.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Run **<INSTALLDIR>**/sap_bobj/serverconfig.sh.
2. Select *1 - Add node*, and press Enter.
3. Type the name of the new node, and press Enter.
4. Type the port number of the new SIA, and press Enter.
5. If prompted, enter the Administrator credentials, the database connection information, the credentials for the system database, and the cluster key.
6. Select *no servers* and press Enter.
7. After the node is created, use the *Server Management* page of the Central Management Console to clone all of the servers from the original node to the new node.

   > **Note**
   >
   > Ensure that the cloned servers have no port conflicts with servers on the old node.

8. Run **<INSTALLDIR>**/sap_bobj/ccm.sh -start **<nodeName>** to start the new node.
9. After the new node has been running for five minutes, use serverconfig.sh to delete the original node.

Related Information

Adding a new node [page 368]
Cloning servers [page 340]
Deleting a node [page 375]

10.12.6 Moving a node

You can move a stopped node from one cluster to another using the Central Configuration Manager (CCM), or using a node management script. Use the following guidelines:

- Ensure that the destination cluster does not have a node with the same name.
- Ensure that all server types installed on the machine where the source node is located are also installed on the destination cluster.
- If you want to add a new machine to a production cluster but do not want the machine to be usable until you finish testing it, install the BI platform on a stand-alone machine, test the machine, then move the node to a production cluster.
- The BI platform version and service pack level for this machine must be consistent with the rest of the cluster.

> **Remember**
>
> You can move a node only on the machine where the node is located.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.12.6.1 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 machine was initially standalone, but it will be added to the destination cluster.

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you move a node.

1. Stop the node in the Central Configuration Manager (CCM).
2. Right-click the node and select *Move*.
3. If prompted, select the data source name, and enter the host name, the port, the database connection information, the Administrator credentials for the destination CMS, and the cluster key.
4. Select a CMS.
   - If your source deployment is running, select *Use existing running CMS*, and click *Next*.
     If prompted, enter the host name and port number for the source system's existing CMS and the Administrator credentials.
   - If your source deployment is stopped, select *Start a new temporary CMS*, and click *Next*.
     If prompted, enter the host name and port number for the source system's temporary CMS, the Administrator credentials, the data source name, the database credentials for the source system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

     > **Caution**
     >
     > Avoid using the deployment while the temporary CMS runs.
5. Review the confirmation page, and click *Finish*.
   The CCM creates a new node on the destination cluster with the same name and the same servers as the node on the source cluster. A copy of the node remains on the source cluster. The configuration templates for the servers in the node do not move. If any errors occur, review the log file.

   > **Caution**
   >
   > Do not use the source cluster after moving the node.
6. In the CCM, start the moved node.

10.12.6.1.1 Moving a node on Windows using a script

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you move a node.

You can use `MoveNode.bat` to move a node on a Windows machine. For more information, see the “Script parameters for moving nodes” section.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Example

Due to the limitations of the command prompt, you must use the caret (^) to escape spaces, the equals sign (=) and the semicolon (;) in these parameters, unless you enclose the text within quotation marks.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

Note

To avoid using the caret in long strings, you can write the script's name and all of its parameters to a temporary `response.bat` file, and then run `response.bat` without any parameters.

Related Information

Variables [page 366]
Script parameters for moving nodes [page 385]

10.12.6.2 To move an existing node on Unix

In this example, the node that you want to move is installed on the source system. The source system machine was initially standalone, but it will be added to the destination cluster.

Caution

Back up the server configuration for the entire cluster before and after you move a node.

1. Run **<INSTALLDIR>**`/sap_bobj/ccm.sh -stop` **<nodeName>** to stop the node.
2. Run **<INSTALLDIR>**`/sap_bobj/serverconfig.sh`
3. Select *4 - Move node*, and press `Enter`.
4. Select the node you want to move, and press `Enter`.
5. When prompted, select the system database connection information, and enter the host name, the port, the Administrator credentials for the destination CMS, and the cluster key.
6. Select a CMS.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- If your source deployment is running, select *existing*, and press Enter.
  If prompted, enter the host name and port number for the source system's existing CMS and the Administrator credentials.
- If your source deployment is stopped, select *temporary*, and press Enter.
  If prompted, enter the host name and port for the source system's temporary CMS, the Administrator credentials, the database connection information and the credentials for the source system database, and the cluster key. A temporary CMS will start. (It will stop when this process finishes.)

> **Caution**
>
> Avoid using the deployment while the temporary CMS runs. Ensure that the existing and temporary CMS use different ports.

7. Review the confirmation page, and press Enter.
   The CCM creates a new node on the destination cluster with the same name and the same servers as the node on the source cluster. A copy of the node remains on the source cluster. The configuration templates for the servers in the node do not move. If any errors occur, review the log file.

> **Caution**
>
> Do not use the source cluster after moving the node.

8. Run `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` to start the moved node.

10.12.6.2.1 Moving a node on Unix using a script

> **Caution**
>
> Back up the server configuration for the entire cluster before and after you move a node.

You can use `movenode.sh` to move a node on a Unix machine. For more information, see the "Script parameters for moving nodes" section.

> **Example**

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Variables [page 366]
Script parameters for moving nodes [page 385]

10.12.7 Script parameters

10.12.7.1 Script parameters for adding, recreating, and deleting nodes

Table 60:

Parameter	Description	Example
`-adopt`	Recreates the node if it already exists in the CMS.	`-adopt`
`-cms`	The name and port number of the Central Management Server (CMS). **Caution** Do not use this parameter if you use `-usetempcms` **Note** You must specify a port number if the CMS is not running on the default 6400 port.	`-cms mycms:6409`
`-cmsport`	• The port number of the CMS when starting a temporary CMS. **Restriction** You must also use the `-usetempcms`, `-dbdriver`, `-connect`, and `-dbkey` parameters. • The port number of the CMS when creating a new CMS. **Restriction** You must also use the `-dbdriver`, `-connect`, and `-dbkey` parameters.	`-cmsport 6401`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description	Example
`-connect`	The connection string of the CMS (or the temporary CMS) system database. **Note** Omit the `HOSTNAME` and `PORT` attributes when connecting to DB2, Oracle, SQL Anywhere, SQL Server, or Sybase databases.	**`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`**
`-dbdriver`	The database driver of the CMS. Accepted values: • **`db2databasesubsystem`** • **`maxdbdatabasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqldatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	The cluster key.	**`-dbkey abc1234`**
`-name`	The name of a node.	**`-name mynode2`**
`-noservers`	Creates a node without servers. **Note** The additional `-createcms` parameter creates a node with a CMS, but no other servers. Omit these parameters to create a node with all of the default servers.	**`-noservers`**
`-password`	The password of the Administrator account.	**`-password Password1`**
`-siaport`	The port number of the Server Intelligence Agent for the node.	**`-siaport 6409`**
`-username`	The user name of the Administrator account.	**`-username Administrator`**
`-usetempcms`	**Caution** Do not use this parameter if you use `-cms` Starts and uses the temporary CMS. **Note** Use a temporary CMS when your deployment is not running.	**`-usetempcms`**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Adding a node on Windows using a script [page 369]
Adding a node on Unix using a script [page 371]
Recreating a node on Windows using a script [page 373]
Recreating a node on Unix using a script [page 375]
Deleting a node on Windows using a script [page 376]
Deleting a node on Unix using a script [page 377]

10.12.7.2 Script parameters for moving nodes

Table 61:

Parameter	Description	Example
`-cms`	The name of the source Central Management Server (CMS). **Caution** Do not use this parameter if you use `-usetempcms` **Note** You must specify a port number if the CMS is not running on the default 6400 port.	`-cms sourceMachine:6409`
`-cmsport`	• The port number of the CMS when starting a temporary CMS. **Restriction** You must also use the `-usetempcms`, `-dbdriver`, `-connect`, and `-dbkey` parameters. • The port number of the CMS when creating a new CMS. **Restriction** You must also use the `-dbdriver`, `-connect`, and `-dbkey` parameters.	`-cmsport 6401`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description	Example
-connect	The connection string of the source CMS (or the temporary CMS) system database. **Note** Omit the HOSTNAME and PORT attributes when connecting to DB2, Oracle, SQL Anywhere, SQL Server, or Sybase databases.	**-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"**
-dbdriver	The database driver of the source CMS. Accepted values: • **db2databasesubsystem** • **maxdbdatabasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqldatabasesubsystem** • **sqlserverdatabasesubsystem** • **sybasedatabasesubsystem** • **newdbdatabasesubsystem**	**-dbdriver mysqldatabasesubsystem**
-dbkey	The source cluster key.	**-dbkey abc1234**
-destcms	The name of the destination CMS. **Note** You must specify a port number if the CMS is not running on the default 6400 port.	**-destcms destinationMachine:6401**
-destconnect	The connection string of the destination CMS system database. **Note** Omit the HOSTNAME and PORT attributes when connecting to DB2, Oracle, SQL Anywhere, SQL Server, or Sybase databases.	**-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Description	Example
-destdbdriver	The database driver of the destination CMS. Accepted values: • **db2databasesubsystem** • **maxdbdatabasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqldatabasesubsystem** • **sybasedatabasesubsystem** • **newdbdatabasesubsystem**	**-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	**Caution** Do not use this parameter if you use -cms Starts and uses the temporary CMS. **Note** Use a temporary CMS when your deployment is not running.	**-usetempcms**

Related Information

Moving a node on Windows using a script [page 380]
Moving a node on Unix using a script [page 382]

10.12.8 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.12.8.1 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.

10.12.9 Changing the user credentials for a node

You can use the Central Configuration Manager (CCM) to specify or update the user credentials for the Server Intelligence Agent (SIA) if the operating system password changes, or if you want to run all of the servers on a node under a different user account.

All servers managed by the SIA run under the same account. To run a server using a non-system account, ensure that your account is a member of the Local Administrators group on the server machine, and that it has the "Replace a process level token" right.

> ⚠ Restriction
>
> On a Unix machine, you must run the BI platform with the same account that was used to install it. To use a different account, reinstall the deployment using a different account.

10.12.9.1 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.13 Renaming a machine in a BI platform deployment

10.13.1 Changing cluster names

The following are best practices for renaming clusters:

> **Caution**
>
> Never deploy multiple clusters with the same name.

Table 62:

Condition	Action
The name of the cluster changes.	Inform your users of the new cluster name and ask them to use it (after the first connection to the CMS using the `<hostname>:<port>` syntax). On the web tier, update the cluster name in the properties files of all web application servers.
You install a different version of the BI platform on a machine that previously ran a CMS, or you add the machine to a different cluster.	• Ensure that the new CMS runs on a different port. • Use different passwords for different clusters to prevent users from logging into an incorrect cluster.

10.13.2 Changing IP addresses

To avoid configuration changes that result from changes to the machine's IP address, select *Server Properties* on the *Servers* tab of the CMC, and then ensure that all servers bind to hostnames, or use the *Auto-Assign* option. In addition, follow these best practices:

Table 63:

Condition	Action
You use ODBC with the CMS database or the auditing database.	Ensure that the DSN uses the CMS database server hostname.
You use another database connection type with the CMS database or the auditing database.	Use the CCM to update the database to use the database server hostname.
The CMS database or the auditing database is located on the same host at the CMS.	Use `localhost` for the machine name.
You use the URL for BI platform web applications that users access using web browsers (for example, the CMC).	Use hostnames instead of IP addresses for the default URL. To update the URL for the default viewer, select *Processing Settings* for the selected application. For example, for Open Document, click the *Applications* tab in the CMC, right-click *Open Document*, and select *Processing Settings*.
You use the URL for BI platform clients based on web services (for example, Crystal Reports for Java or LiveOffice).	
You use OpenDocument.	

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Alternative guidelines

> **Note**
>
> Follow these guidelines only if you cannot follow the best practices described above.

Table 64: For machines hosting servers

Condition	Action
The host contains BI platform servers, and the servers must bind to specific IP addresses.	Change the IP addresses on the *Servers* tab of the CMC, but do not restart the servers until everything on the machine has been updated. Then reboot the machine; not the individual BI platform servers.
A database connection must use an IP address.	Change the IP address.
An IP address change is required in a static IP network.	Change the IP address of the BI platform machine. **Tip** Log on to the CMC to verify that the BI platform is operational.

> **Remember**
>
> Restart the machine after performing an action.

Table 65: For machines hosting the web application server

Condition	Action
The OpenDocument default viewer URL must use an IP address.	Update the IP address in the *Default Viewer URL* field in the *Processing Settings* section of the *Applications* tab of the CMC.
Your users access BI platform web applications (for example, the CMC) by providing a URL with an IP address in their browsers.	Inform your users of the new IP address.
BI platform clients based on web services (for example, Crystal Reports for Java, or LiveOffice) must use IP addresses.	Configure all clients to use the new IP address.

Related Information

Selecting a new or existing CMS database [page 398]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.13.3 Renaming machines

You can rename machines in a BI platform deployment at any time by stopping all BI platform servers on the machine and then renaming the machine. The following are best practices for renaming machines:

Table 66:

Condition	Action
You log on for the first time.	Use the CMS machine name (rather than the cluster name).
You have a multi-machine deployment.	Ensure that all CMS servers on all other machines are running during renaming.

10.13.3.1 Server tier

> **Note**
>
> Before you rename the CMS machine, inspect the configuration of all servers located on the machine that you would like to rename on the "Server Management" tab of the CMC. If the *Hostname* property uses the old CMS hostname, update it to the new CMS hostname.

> **Remember**
>
> Do not restart the servers until you complete all machine renaming procedures.

Follow these instructions for renaming server tier machines:

Table 67:

Condition	Action
The renamed machine hosts a CMS, and users have previously logged in by providing the name of the old machine.	Inform your users of the CMS machine name and ask them to use it.
The renamed machine hosts a CMS, and the BI platform web application default properties files contain the old CMS hostname in the `cms.default` property.	Update the CMS machine name in the `cms.default` property in all custom property files on all web tier machines. On Tomcat, the property files that you create are located in **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` by default. **Note** If no custom property files exist, create new custom property files. Copy the the default property files to a custom folder, and remove all content except for the `cms.default` line from the custom property files.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Condition	Action
The renamed machine hosts a CMS, and SAP BusinessObjects Explorer is installed on any machine in the cluster.	Replace the old CMS hostname with the new hostname in the `default.cms.name` property in the `default.settings.properties` file on all machines that host web application servers. By default, on Tomcat, the `default.settings.properties` file is located in **`<INSTALLDIR>`**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\` **Remember** Restart the Explorer web application or application server after performing the action.
You use SSO with Explorer	Update the `cms` value in `jsp-sso-provider.jsp` and update the `sso.global.cms` and `sso.trusted.auth.x509.cms` values in `sso.properties` to the new CMS hostname.
You use Portal Integration Kits or custom applications.	Configure the Portal Integration Kits or custom applications to use the new CMS hostname.
Your deployment meets all of the following conditions: • A cluster has multiple nodes. • All CMS servers run only on the machine that has been renamed. • At least one node does not host the CMS. • You rename a machine with at least one node. • The IP address changes during the renaming process.	Use the CCM to perform the "Recreate Node" workflow on all nodes, except for the node that hosts the CMS, and then start all BI platform nodes in the deployment. For more information, see the "Managing Nodes" chapter.

Remember

Restart the web application or application server after performing an action.

Related Information

Recreating a node [page 372]

10.13.3.2 Web tier

If you rename the machine that hosts the BI platform web application server, follow these instructions:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 68:

Condition	Action
You change the name of the machine that hosts the BI platform web application server, and the URL of the default OpenDocument viewer uses a web application server hostname.	Log onto the CMC and update the default viewer URL in *Applications* > *CMC* > *Processing Settings*.
You change the name of the machine that hosts the BI platform web application server, and your users access BI platform web applications using a URL that includes a web application server hostname.	Ask your users to access BI platform web applications using a URL that includes the new web application server hostname.
You change the name of the machine that hosts the BI platform web application server, and web service-based BI platform clients use web application server hostnames in the URL.	Reconfigure all web-service-based BI platform clients to use the new web application server hostname.

10.13.3.3 Databases

If you rename the machine hosting the CMS system database or the auditing database, follow these best practices:

Table 69:

Condition	Action
You want to avoid updating the IP address.	Use the CMS database or auditing database machine name in the data source name (DSN).
The CMS database or auditing database is located on the same host as the CMS.	Use `localhost` in the DSN to avoid updating it if the hostname changes.

CMS system database

Table 70:

Condition	Action
You rename a machine that hosts the CMS system database, and you use ODBC.	Update the CMS database DSN to the new database server hostname.
You rename a machine that hosts the CMS system database, and you use a non-ODBC connection type.	Use the CCM to update the CMS database to the new database server hostname on every node in the cluster.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Auditing database

Table 71:

Condition	Action
You rename a machine that hosts the auditing database, and you use ODBC.	Update the auditing database DSN to use the new database server hostname.
You rename a machine that hosts the auditing database, and you use a non-ODBC connection type.	Update the database server machine name to the new database server hostname on the *Auditing* tab of the CMC.

10.13.3.4 File Repository Servers

If you rename the machine that hosts the FRS file store, you must update the *Input File Repository* and *Output File Repository* servers on the "Server Management" page of the CMC, and ensure that the *File Store Directory* and *Temporary Directory* properties use the new file store path, and then restart the servers.

10.14 Using 32-bit and 64-bit third-party libraries with BI platform

BI platform servers are a combination of 32-bit and 64-bit processes. Some servers additionally launch 32-bit and 64-bit child processes. To use the correct version of third-party libraries (32-bit vs 64-bit) with BI platform processes, you must set separate 32-bit and 64-bit environment variables on the machines hosting the BI platform. You must then set an additional environment variable that contains a comma-separated list of those environment variables that have 32-bit and 64-bit versions. When a process is launched by the BI platform, it will select the appropriate variable depending on whether the process is 32-bit or 64-bit.

- **<FIRST_ENV_VAR>**=The value to be used by 64-bit BI platform processes.
- **<FIRST_ENV_VAR32>**=The value to be used by 32-bit processes.
- **<SECOND_ENV_VAR>**=The value to be used by 64-bit processes.
- **<SECOND_ENV_VAR32>**=The value to be used by 32-bit processes.
- BOE_USE_32BIT_ENV_FOR=**<FIRST_ENV_VAR>**,**<SECOND_ENV_VAR>**

For example, if you've installed the BI platform on an AIX machine, as well as 32-bit and 64-bit Oracle clients, and need to set the LIBPATH variable, set the following variables:

- ORACLE_HOME=**<home directory of the 64-bit version of the Oracle client>**
- ORACLE_HOME32=**<home directory of the 32-bit version>**
- LIBPATH=**<library path of the 64-bit version>**
- LIBPATH32=**<library path of the 32-bit version>**
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **Note**
>
> In Linux and Solaris, do not use BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH to separate the 32-bit and 64-bit paths. Instead, add both 32-bit and 64-bit paths to LD_LIBRARY_PATH.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10.15 Managing server and node placeholders

10.15.1 To view server placeholders

In the *Servers* management area of the CMC, right-click a server and select *Placeholders*.
The *Placeholders* dialog displays a list of placeholders for all of the servers on the same cluster as the server that you selected. If you want to change the value for a placeholder, modify the placeholder for the node.

Related Information

Server and node placeholders [page 921]

10.15.2 To view and edit the placeholders for a node

1. In the *Servers* management area of the Central Management Console, right-click the node for which you want to change the placeholders, and select *Placeholders*.
2. If you want to edit any of the settings for the placeholders, make the appropriate changes and click *Save* to continue.

Related Information

Server and node placeholders [page 921]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

11 Managing Central Management Server (CMS) Databases

11.1 Managing CMS system database connections

If the CMS system database is unavailable, for example due to a hardware or software failure or a network problem, the CMS goes into the "Waiting for resources" state. If the BI platform deployment has multiple CMSs, then subsequent requests from other servers are forwarded to any CMSs in the cluster that have an active connection to the system database. While a CMS is in the "Waiting for resources" state, any current requests that do not require database access continue to be processed, but requests that require access to the CMS database will fail.

By default, a CMS in the "Waiting for resources" state periodically attempts to reestablish the number of connections that are specified in the "System Database Connections Requested" property. As soon as at least one database connection is established, the CMS synchronizes all necessary data, goes into the "Running" state, and resumes normal operations.

In some cases, you may want to prevent the CMS from automatically reestablishing a connection to the database. For example, you may want to verify the integrity of the database before database connections are reestablished. To do so, on the *Properties* page of the CMS server, uncheck *Auto Reconnect to System Database*.

Related Information

To change a server's properties [page 355]

11.1.1 To select SQL Anywhere as a CMS database

To use SQL Anywhere as a CMS database, you must perform the following steps:

1. Stop all nodes in the system.
2. Run the appropriate application:
   - On Unix, run `./cmsdbsetup.sh`.
   - On Windows, start the Central Configuration Manager (CCM).
3. Copy your data from the default CMS database, selecting SQL Anywhere as the destination database. For more information, see the related link "Copying data from one CMS system database to another".
4. On multi-node deployments, update the CMS data source on every node (except the node on which you copy the database) to the new SQL Anywhere database. For more information, see the related link "Selecting a new or existing CMS database".
5. Ensure that the deployment is operational (for example, log into the CMC and view a report).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Copying data from one CMS system database to another [page 402]
Selecting a new or existing CMS database [page 398]

11.1.2 To select SAP HANA as a CMS database

To use SAP HANA as a CMS database, you must perform the following steps.

1. Install the BI platform with the default CMS database.
2. Install the SAP HANA client.
3. Create a connection to SAP HANA.
   - On Unix, check the environment variable `ODBCINI`. If the variable exists and points to an existing `odbc.ini` file, add the following lines to that file:

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>

     [NewDB]
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     ```

     `<New_DB_version>` is the SAP HANA version; for example "NewDB 1.0", `<HANA Server IP address>` is the SAP HANA server IP address, and `<HANA server port #>` is the SAP HANA server port number. If the `ODBCINI` environment variable does not exist, create an `odbc.ini` file in the **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/` directory, add the above lines to the file, and set the `ODBCINI` environment variable as follows:

     ```
     ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

   - On Windows, create an ODBC connection to SAP HANA.

     > **Note**
     >
     > For ODBC connection changes, be sure to run the 64-bit version of the ODBC Data Source Administrator: *Start* > *Control Panel* > *Administrative Tools* > *Data Sources (ODBC)*.

4. Ensure that connections can be made to the SAP HANA server.
   - On Unix, you can test the connection to the SAP HANA server by running the following command. The variables in the following example refer to the SAP HANA installation:

     ```
     <INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID> <NONADMINUSER>
     <NONADMINPASSWORD>
     ```

   - On Windows, you can use the ODBC Data Source Administrator to test the SAP HANA ODBC connection.
5. On Unix, copy `libodbcHDB.so` from the SAP HANA installation directory to **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/`**<PLATFORM>**
6. Stop all nodes in the system.
7. Run the appropriate application:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- On Unix, run `./cmsdbsetup.sh`.
- On Windows, start the Central Configuration Manager (CCM).

8. Copy your data from the default CMS database, selecting SAP HANA as the destination database. For more information, see the related link “Copying data from one CMS system database to another”.
9. On multi-node deployments, update the CMS data source on every node (except the node on which you copy the database) to the new SAP HANAdatabase. For more information, see the related link “Selecting a new or existing CMS database”.
10. Ensure that the deployment is operational (for example, log into the CMC and view a report).

Related Information

Copying data from one CMS system database to another [page 402]
Selecting a new or existing CMS database [page 398]

11.2 Selecting a new or existing CMS database

You can use the CCM or `cmsdbsetup.sh` to specify a new or existing CMS system database for a node. Generally, there are only a few times when you need to complete these steps:

- If you have changed the password for the current CMS system database, these steps allow you to disconnect from, and then reconnect to, the current database. When prompted, you can provide the CMS with the new password.
- If you want to select and initialize an empty database for the BI platform, these steps allow you to select that new data source.
- If you have restored a CMS system database from backup (using your standard database administration tools and procedures) in a way that renders the original database connection invalid, you will need to reconnect the CMS to the restored database. (This might occur, for instance, if you restored the original CMS database to a newly installed database server.)

> **Note**
>
> If you use IBM DB2 as your CMS database, and upgrade it from a version older than 9.5 Fix Pack 5 to version 9.5 Fix Pack 5 or newer (for the 9.5 line), or if you upgrade from a version older than 9.7 Fix Pack 1 to version 9.7 Fix Pack 1 or newer (for the 9.7 line), then during the next restart of the BI platform node or CMS, the CMS database schema will automatically be updated by the CMS to support HADR-compatible schema.
>
> This may be a lengthy process, during which the BI platform system will not be available for use. Do not interrupt the update process, to avoid corrupting the CMS database. It is highly recommended that you back up your CMS database before performing this operation. Also, do not try to use IBM HADR with an IBM DB2 CMS database of a version older than 9.5 Fix Pack 5 (for the 9.5 line) or 9.7 Fix Pack 1 (for the 9.7 line).

> **Note**
>
> Do not configure a BI platform installation to use a CMS system database belonging to a different cluster, unless you are performing a system copy workflow.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

System corruption may occur if the versions and patch levels of the BI platform installations and CMS databases are different, or if installation paths differ, or if installed components differ, etc.

To prevent corruption, do not attempt to migrate BI content from one system to another by pointing the BI platform deployment to a CMS database of another BI platform system, especially one of a different version and patch level.

11.2.1 To select a new or existing CMS database on Windows

1. Use the CCM to stop the Server Intelligence Agent (SIA).
2. Select the SIA and click the *Specify CMS Data Source* button.
3. Select *Update Data Source Settings* and click *OK*.
4. Select a database driver and click *OK*.
5. These steps depend upon the connection type you selected:
   - If you selected ODBC, the Windows "Select Data Source" dialog box appears. Select the ODBC data source that you want to use as the CMS database; then click *OK*. (Click *New* to configure a new DSN.) When prompted, provide your database credentials and click *OK*.
   - If you selected a native driver, you are prompted for your database Server Name, your Login ID, and your Password. Provide this information and then click *OK*.
6. Specify the cluster key.
7. Restart the Server Intelligence Agent.

11.2.2 To select a new or existing CMS database on UNIX

Use the `cmsdbsetup.sh` script. For reference, see the "Unix scripts" topic in the Command Line Administration chapter in the *BI platform Administrator Guide*.

1. Run the `cmsdbsetup.sh` script (located by default in **`<INSTALLDIR>`**`/sap_bobj/`).
2. Select the update action (option 6).
3. When prompted, provide the database type of the new CMS database.
4. Provide the database information (for example: host name, user name, password, and cluster key).
   A notification message appears when the CMS database has been pointed to the new location.
5. If you are prompted to rebuild the Server Intelligence Agent (SIA), provide the administrator password and the port number you want the CMS to communicate on.

> **Note**
>
> You will be prompted for this information only if you point to an empty CMS database.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Unix scripts [page 807]

11.3 Recreating the CMS system database

This procedure shows how to recreate (reinitialize) the current CMS system database. By performing this task, you destroy all data that is already present in the database. This procedure is useful, for instance, if you have installed the BI platform in a development environment for designing and testing your own, custom web applications. You can reinitialize the CMS system database in your development environment every time you need to clear the system of all its data.

> **Caution**
>
> By implementing the steps outlined in this workflow, you will delete all data in the CMS database as well as objects such as reports and users. Do not perform these steps on a production deployment.

It is very important that you back up all server configuration settings before reinitializing the CMS system database. When you recreate the database, your server configuration settings will be erased and you must have a backup in order to restore this information.

When you recreate the system database, your existing license keys should be retained in the database. However, if you need to enter license keys again, log on to the CMC with the default Administrator account. Go to the Authorization management area and enter your information on the License Keys tab.

> **Note**
>
> If you reinitialize your CMS system database, all data in your current CMS system database will be destroyed. Consider backing up your current database before beginning. If necessary, contact your database administrator.

Related Information

Backing up server settings [page 448]

11.3.1 To recreate the CMS system database on Windows

1. Use the CCM to stop the Server Intelligence Agent (SIA).

   > **Note**
   >
   > For this procedure, you cannot run the CCM on a remote machine; it must be run on a machine with at least one valid node. Also, the CMS binaries must be installed on this machine.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Right-click the SIA and choose *Properties*.
3. In the *Properties* dialog box, go to the *Configuration* tab and click *Specify*.
4. In the *CMS Database Setup* dialog box, click *Recreate the current Data Source*.

   > **Note**
   >
   > Servers and objects from the machine where you ran the CCM in step 1 will also be recreated. However, not all objects will be recreated; only the key default objects. For example, sample reports are not recreated.

5. Click *OK* and, when prompted to confirm, click *Yes*.
6. Specify the password for the CMS system database, and click *OK*.

   > **Note**
   >
   > Ensure that you set a new administrator password. By default, the Administrator account will have no password.

   The CCM notifies you when the CMS system database setup is complete.
7. Click *OK*.

   You are returned to the CCM.
8. Restart the Server Intelligence Agent and enable services.

   While it is starting, the Server Intelligence Agent starts the CMS. The CMS writes required system data to the newly emptied data source.
9. If your deployment has more than one machine, you need to re-create the nodes on the other machines.

11.3.2 To recreate the CMS system database on UNIX

Use the `cmsdbsetup.sh` script. For reference, see the “Unix scripts” topic in the Command Line Administration chapter in the *BI platform Administrator Guide*.

1. Run `cmsdbsetup.sh` (located in **`<INSTALLDIR>`**`/sap_bobj/`, by default).
2. Select the "reinitialize" option (option 5), then confirm your choice.
   The `cmsdbsetup.sh` script begins recreating the CMS system database.
3. Provide the CMS system database password.
4. When the database creation is complete, exit the `cmsdbsetup.sh` script.
5. Provide the database information (for example: host name, user name, and password).
   A notification message appears when the CMS database has been pointed to the new location.
6. If you are prompted to rebuild the Server Intelligence Agent (SIA), provide the administrator password and the port number you want to CMS to communicate on.

   > **Note**
   >
   > You will be prompted for this information only if you point to an empty CMS database.

7. In the **`<INSTALLDIR>`**`/sap_bobj/` directory, use the following command to start the node.

   ```
   ccm.sh -start <nodename>
   ```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8. To enable the services, use the following command:

```
ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password
<password>
```

> **Note**
>
> Since you just recreated the CMS database, the administrator password is blank.

Related Information

Unix scripts [page 807]

11.4 Copying data from one CMS system database to another

You can use the Central Configuration Manager (CCM) or `cmsdbsetup.sh` to copy system data from one database server into another database server. For example, if you want to replace the database with another database because you are upgrading the database or are moving from one database type to another, you can copy the contents of the existing database into the new database before decommissioning the existing database.

The destination database is initialized before the new data is copied in, so any existing contents of the destination database are permanently deleted (all BI platform tables are destroyed permanently and then recreated). Once the data has been copied, the destination database is established as the current database for the CMS.

> **Note**
>
> If you want to import users, groups, folders, and reports from a previous major version of the BI platform to the current major version, use the upgrade management tool. For more information, see the *SAP BI platform Upgrade Guide*.

> **Caution**
>
> Never attempt to use a CMS database from another BI platform cluster. Before starting this workflow, always ensure that the source CMS database was used with this BI platform cluster, and not with another BI platform cluster.

> **Caution**
>
> Never attempt to perform an upgrade by using the CMS database copy workflow. The CMS database copy workflow is designed for moving a CMS database from one database server to another database server. It is not designed for upgrading the CMS database. Before starting this workflow, always ensure that the source CMS database was used with this BI platform cluster, and that it has the same version and patch levels as the current BI platform installation.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

11.4.1 Preparing to copy a CMS system database

Before copying a CMS system database, take the source and the destination environments offline by disabling and subsequently stopping all servers. Back up both CMS databases, and back up the root directories used by all Input and Output File Repository Servers. If necessary, contact your database or network administrator.

Ensure that you have a database user account that has permission to read all data in the source database, and a database user account that has Create, Delete, and Update rights to the destination database. Also ensure also that you can connect to both databases—through your database client software or through ODBC, according to your configuration—from the CMS machine whose database you are replacing.

If you are copying a CMS database from its current location to a different database server, your current CMS database is the source environment. Its contents are copied to the destination database, which is then established as the active database for the current CMS. This is the procedure to follow if you want to move the default CMS database from the existing default database to a dedicated database server, such as Microsoft SQL Server, Informix, Oracle, DB2, or Sybase. Log on with an administrative account to the machine that is running the CMS whose database you want to move.

> **Note**
>
> When you copy data from one database to another, the destination database is initialized before the new data is copied in. That is, if your destination database does not contain the BI platform system tables, these tables are created. If the destination database does contain the BI platform system tables, the tables will be permanently deleted, new system tables will be created, and data from the source database will be copied into the new tables. Other tables in the database are unaffected.

> **Note**
>
> If you are copying a CMS system database to a MaxDB destination database on Windows, you must ensure that the path to the MaxDB client has been added to the **<PATH>** environment variable. For example, `;C:\Program Files\sdb\MAXDB1\pgm`.

11.4.2 To copy a CMS system database on Windows

Before you copy the contents of the CMS database, ensure that you can logon to the destination database with an account that has permissions to add or drop tables, and to add, drop, or modify data in those tables.

1. Open the Central Configuration Manager (CCM) and stop the Server Intelligence Agent (SIA).
2. Right-click the SIA and choose *Properties*.
3. Click the *Configuration* tab, and then click *Specify*.
4. Choose *Copy*, then click *OK*.
5. Select the database type for the source CMS database, and then specify its database information (including host name, user name, and password).
6. Select the database type for the destination CMS database, and then specify its database information (including host name, user name, and password).
7. When the CMS database has finished copying, click *OK*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

11.4.3 To copy data from a CMS system database on UNIX

Before you copy the contents of the CMS database, ensure that you can logon to the destination database with an account that has permissions to add or drop tables, and to add, drop, or modify data in those tables.

> **Note**
>
> On UNIX you can not migrate directly from a source environment that uses an ODBC connection to the CMS database. If your source CMS database uses ODBC, you must first upgrade that system to a supported native driver.

1. Stop the CMS by typing the following command:
   ```
   ./ccm.sh -stop <nodename>
   ```
2. Run `cmsdbsetup.sh` (located in **<INSTALLDIR>**`/sap_bobj/`, by default).
3. Select the "copy" option (option 4), then confirm your choice.
4. Select the database type for the source CMS database, then specify its database information (including host name, user name, and password).
5. Select the database type for the destination CMS database, and then specify its database information (including host name, user name, and password).
   The CMS database is copied to the destination database. A message appears when the copy is complete.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12 Managing Web Application Container Servers (WACS)

12.1 WACS

12.1.1 Web Application Container Server (WACS)

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

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

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

12.1.1.1 Do I need WACS?

If you do not want to use a Java application server to host your SAP BusinessObjects web applications, then you can host them on WACS.

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

12.1.1.2 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 BI platform servers.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.1.3 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.	• Adding or removing additional WACS to your deployment [page 407] • Cloning a Web Application Container Server [page 409]
How can I improve the availability of my web-tier?	Create additional WACS in your deployment, so that in the event of a hardware or software failure on one server, another server can continue servicing requests.	Adding or removing additional WACS to your deployment [page 407]
How can I create an environment where I can easily recover from a misconfigured CMC?	Create a second, stopped, WACS, and use this WACS to define a configuration template. In the event that the primary WACS becomes misconfigured, either use the second WACS until you configure the first server, or apply the configuration template to the first server.	Adding or removing additional WACS to your deployment [page 407]
How can I improve the security of communication between clients and WACS?	Configure HTTPS on WACS.	• Configuring HTTPS/SSL [page 412] • Using WACS with firewalls [page 435]
How can I improve the security of communication between WACS and other BI platform servers in my deployment?	Configure SSL communication between WACS and other BI platform servers in your deployment.	• Configuring servers for SSL [page 156] • Using WACS with firewalls [page 435]
Can I use WACS with HTTPS and a reverse proxy?	You can use WACS with HTTPS and a reverse proxy if you create two WACS and configure both servers with HTTPS. Use the first WACS for communication inside your internal network, and the other WACS for communication with an external network through a reverse proxy.	To configure WACS to support HTTPS with a reverse proxy [page 435]
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.	• Using WACS with other web servers [page 434] • Using WACS with a load balancer [page 434] • Using WACS with a reverse proxy [page 434] • Using WACS with firewalls [page 435]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Task	Description	Topic
Can I use WACS in a deployment with a load balancer?	You can use WACS in a deployment that uses a hardware load balancer. WACS itself cannot be used as a load balancer.	Using WACS with a load balancer [page 434]
Can I use WACS in a deployment with a reverse proxy?	You can use WACS in a deployment that uses a reverse proxy. WACS itself cannot be used as a reverse proxy.	Using WACS with a reverse proxy [page 434]
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.	• To configure tracing on WACS [page 437] • To view server metrics [page 437]
I don't get any pages served to me on a particular port. What is wrong?	There are a number of reasons why you might not be able to connect to WACS. Check to see if: • The HTTP, HTTP through proxy, and HTTPS ports that you specified for the WACS have been taken by other applications. • The WACS has enough memory allocated to it. • The WACS allows enough concurrent requests. • If necessary, restore the system defaults for the WACS.	• To resolve HTTP port conflicts [page 438] • To change memory settings [page 439] • To change the number of concurrent requests [page 439] • To restore system defaults [page 440]
How can I configure the properties of web applications that are hosted on WACS?	The procedure for configuring the properties for web applications depends on the specific property and web application. For more information, see the "Configuring web application properties" section of this chapter.	Configuring web application properties [page 436]
Where can I find a list of WACS properties?	The "Server Properties Appendix" of this guide contains a list of WACS properties.	Core Services properties [page 869]

12.1.2 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:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- 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.

12.1.2.1 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 BI platform installation program. There are two ways that you can install WACS:

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

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

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

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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.2.2 Adding a new Web Application Container Server

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

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

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

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

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

12.1.2.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **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 Information

To resolve HTTP port conflicts [page 438]

12.1.2.4 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*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.3 Adding or removing services to WACS

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

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

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

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

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

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

12.1.3.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

12.1.4 Configuring HTTPS/SSL

You can use the Secure Sockets Layer (SSL) protocol and HTTP for network communication between clients and WACS in your BI platform deployment. SSL/HTTPS encrypts network traffic and provides improved security.

There are two types of SSL:

- SSL used between BI platform servers, including WACS and other BI platform servers in your deployment. This is known as CORBA SSL. For more information on using SSL between the BI platform servers in your deployment, see the "Understanding communication between SAP BI platform components" section of the "Working with Firewalls" chapter of the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.
- HTTP over SSL, which occurs between WACS and clients (for example, browsers) that communicate with WACS.

> **Note**
>
> If you are deploying WACS in a deployment with a proxy or reverse proxy, and want to use SSL to secure the network communication in your deployment, you must create two WACS. For more information, see *Using WACS with a reverse proxy*.

To configure HTTPS/SSL on a WACS, you must 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 PCKS12 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 Information

Understanding communication between BI platform components [page 165]
Using WACS with a reverse proxy [page 434]

12.1.4.1 To generate a PKCS12 certificate file store

There are many ways of generating a PKCS12 certificate file store or Java keystore, and tools that you can use. The method that you use depends on the tools that you have access to and are familiar with.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This example demonstrates how to generate a PKCS12 file using Microsoft's Internet Information Services (IIS) and the Microsoft Management Console (MMC), for Windows Server 2008.

1. Log on to the machine that hosts WACS as an administrator.
2. In IIS, request a certificate from the 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 the Certificates Snap-in to the MMC:
   a. From the *File* menu, click *Add/Remove Snap-in*.
      The *Add or Remove Snap-ins* screen appears.
   b. From the *Available snap-ins* list, select *Certificates*, and click *Add*.
   c. Select *Computer account*, and click *Next*.
   d. Select *Local Computer*, and click *Finish*.
   e. 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.

12.1.4.2 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*.
   b. In the *Available snap-ins* list, select *Internet Information Services (IIS) Manager*, and click *Add*.
   c. Click *OK*.
      The IIS snap-in is added to the MMC.
4. Follow the steps described here to create a certificate trust list: http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard .

12.1.4.3 To configure HTTPS/SSL

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

    > **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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **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.

12.1.5 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

12.1.6 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).

If you are configuring single sign on through AD Kerberos for Web Services SDK and QaaWS, you must also configure both WACS and the machine that is hosting WACS.

Related Information

Windows AD security plug-in [page 239]
To map Windows AD users and groups [page 240]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting up a service account for AD authentication with Kerberos [page 238]
Running the SIA under the BI platform service account [page 245]
Enabling Kerberos authentication in the Windows AD plug-in for WACS [page 416]
Creating configuration files [page 417]
Configuring WACS for AD Kerberos [page 420]
Configuring AD Kerberos single sign-on [page 422]

12.1.6.1 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.

- Enabling Kerberos authentication and single sign-on, if single sign-on is desired.
- Entering the service principal name (SPN) for the service account.

12.1.6.1.1 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 [page 238]
- Running the SIA under the BI platform service account [page 245]
- To map Windows AD users and groups [page 240]

12.1.6.1.2 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. Ensure that the *Enable Windows Active Directory (AD)* check box is selected.
4. Under *Authentication Options*, select *Use Kerberos authentication*.
5. If you want to configure single sign-on to a database, select the *Cache security context* (required for SSO to database) check box.
6. In the *Service principal name* field, enter the account and domain of the service account or the SPN mapping to the service account.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Use the following format, where **<svcacct>** is the name of the service account or SPN you created earlier, and **<DNS.COM>** is your fully qualified domain in uppercase. For example, the Service Account would be svcacct@DNS.COM and the SPN would be BOBJCentralMS/some_name@DOMAIN.COM.

> **Note**
>
> - If you plan to allow users from other domains than the default domain to log on, you must provide the SPN you mapped earlier.
> - The service account is case sensitive. The case of the account you enter here must match with what is set up in your Active Directory Domain.
> - This must be the same account that you use to run the BI platform servers or the SPN that maps to this account.

7. If you want to configure single sign-on, select *Enable Single Sign On for selected authentication mode*.

> **Note**
>
> If you selected to enable single sign-on, you will need to configure the WACS.

Related Information

Configuring AD Kerberos single sign-on [page 422]

12.1.6.2 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.

12.1.6.2.1 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:\Windows` for Windows.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **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.

> **Note**
>
> `kdc` is the Host name of the Domain Controller.

> **Note**
>
> 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 [page 419].

> **Note**
>
> 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.6.2.2 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:\Windows`.

   > **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.

12.1.6.2.3 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
        }
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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
        }
```

12.1.6.3 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).

12.1.6.3.1 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.

12.1.6.4 Troubleshooting Kerberos

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Kerberos configuration

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.6.4.1 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.

12.1.6.4.2 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.

```
<INSTALLDIR>\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.

12.1.6.4.3 Mapped AD user unable to log on to the BI platform on WACS

The following two issues may occur, despite the fact that the users have been mapped to the BI platform.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.6.4.3.1 Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to the BI platform. Despite this fact, they are unable to successfully log 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.

12.1.6.4.3.2 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.

12.1.7 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, you must ensure that you have configured both the WACS and the machine that is hosting WACS for AD Kerberos authentication.

To configure WACS for AD Kerberos single sign-on, you must first configure the machine that is hosting WACS, and then configure the WACS itself.

> **Note**
>
> If you plan to use single sign-on in a reverse proxy environment, read the security information in this guide.

Related Information

Security overview [page 137]
Configuring AD Kerberos for WACS [page 415]

 © 2015 SAP SE or an SAP affiliate company. All rights reserved.

Configuring your machine for AD Kerberos single sign-on [page 423]
Configuring WACS for AD Kerberos single sign-on [page 423]

12.1.7.1 Configuring your machine for AD Kerberos single sign-on

To configure AD Kerberos single sign-on for Web Services SDK and QaaWS, you must first configure the machine that is hosting WACS:

- To configure constrained delegation for Vintela SSO [page 258]
- To set up the service account for Vintela SSO [page 257]
- Setting up multiple SPNs [page 423]
- To increase the header size limit of your WACS [page 423]

The following sections describe how to complete each of these steps.

12.1.7.1.1 Setting up multiple SPNs

Using multiple SPNs is not supported.

12.1.7.1.2 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 users. 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.

12.1.7.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.

12.1.7.3 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 the BI platform 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 [page 422].

12.1.7.3.1 To enable single sign-on to the database

1. Open the `krb5.ini` file that is being used for your deployment of the BI platform.

   The default location for this file is the C:\Windows 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.8 Configuring RESTful web services

The Business Intelligence platform RESTful web services SDK allows you to access the BI platform using the HTTP protocol. This enables users to navigate the BI platform repository and schedule objects using any programming language that supports HTTP requests. RESTful web services are installed as part of WACS.

This section explains how to administer RESTful web services. For more information about RESTful web services, see the *Business Intelligence platform RESTful Web Service Developer Guide*.

12.1.8.1 Applications

12.1.8.1.1 To configure the base URL for RESTful web services

If your BI platform deployment uses a proxy server or contains more than one instance of the Web Application Container Server (WACS), you may need to configure the base URL for use with RESTful web services. Before you configure the base URL, you must know the server name and port number that listens to RESTful web service requests.

The base URL is used as part of every RESTful web service request. Developers programmatically discover the base URL and use it to direct RESTful web service requests to the correct server and port. The base URL is also used in RESTful web service responses to define hyperlinks to other RESTful resources.

> **Note**
>
> In default installations of the BI platform, the base URL is defined as `http://<servername>:6405/biprws`. Replace `<servername>` with the name of the server that hosts RESTful web services.

1. Log on to the Central Management Console (CMC) as an administrator.
2. In the CMC, click *Applications*.
   A list of applications is displayed.
3. Right-click *RESTful Web Service* > *Properties*.
   The *Properties* dialog box appears.
4. In the *Access URL* text box, type the name of the base URL for RESTful web services.
   For example, type `http://<servername>:<portnumber>/biprws`. Replace `<servername>` and `<portnumber>` with the name of the server and the port that listens to RESTful web service requests.
5. Click *Save and Close*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.8.2 WACS Properties

12.1.8.2.1 To configure Methods and Headers command line parameters

As an administrator, you can restrict what methods and headers may be used by RESTful web services, by adding the appropriate options to *Command Line Parameters* in the properties of your Web Application Container Service (WACS). Changes to the parameters require restarting the WACS service.

1. Log on to the Central Management Console as an administrator user.
2. Click *Servers*, and then click *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.
4. In the *Command Line Parameters* area, enter the methods and headers that will be allowed.
   Each option group is enclosed by double quotes. Use Methods other than `GET`, `HEAD` and `POST`. Use commas to separate the option values such as `PUT` and `DELETE` as shown in the following example.

   ```
   "-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
   "-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-
   Authenticate"
   ```

   > **Note**
   >
   > The default value to allow all methods and headers is `*` (asterisk). Omitting the command line parameters entirely, has the same effect.

5. Click *Save and Close*.
6. Restart the service by right-clicking on the WACS server name, for example `MySIA.WebApplicationContainerServer` and click *Restart Server*.

12.1.8.2.2 System Property Configuration

12.1.8.2.2.1 To enable the error message stack

As an administrator, you can configure the error messages returned by RESTful web services to include the error stack. The error stack provides extra debugging information that can be used to discover where errors have occurred.

> **Note**
>
> You may not want to enable the error stack in production scenarios, because it could provide information about the BI platform that you do not want to reveal to end users. It is recommended to enable the error stack in production scenarios as required for debugging, and to turn it off when it is no longer needed.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Log on to the Central Management Console as administrator user.
2. Click *Servers*, and then click *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, right-click on `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.
4. In the *RESTful Web Service* area, select *Show Error Stack*.
5. Click *Save and Close*.

Error stack information is included in RESTful web service error messages.

12.1.8.2.2.2 To set the default number of entries displayed on each page

When a RESTful web service response contains a feed with a large number of entries, the response can be divided into pages. You can configure the default number of entries that are displayed on each page. When developers make RESTful web service requests, they can specify the number of entries to display on each page. However, if they do not specify this value then the default page size is used.

1. Log on to the Central Management Console as an administrator.
2. Click *Servers*, and then click *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, right click on `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.
4. In the *RESTful Web Service* area, type the default page size in the *Default Number of Objects on One Page* text area.
5. Click *Save and Close*.

12.1.8.2.2.3 To set the timeout value of a logon token

Logon tokens expire after they have not been used for a certain amount of time. You can set the amount of time that an unused logon token remains valid.

> **Note**
>
> By default, the logon token timeout value is one hour.

1. Log on to the Central Management Console as an administrator.
2. Click *Servers*, and then click *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, right click on `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.
4. In the *RESTful Web Service* area, type the number of minutes for a logon token to be valid in the *Enterprise Session Token Timeout (minutes)* text area.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. Click *Save and Close*.

12.1.8.2.2.4 To configure session pool settings

You can improve server performance by using a session pool. The session pool caches active RESTful web service sessions so they can be reused when a user sends another request that uses the same logon token in the HTTP request header. The session pool size defines the number of cached sessions to be stored at one time, and the session timeout value controls the amount of time that a session is cached.

You can set the session pool size and the session timeout value:

1. Log on to the Central Management Console (CMC) as an administrator.
2. Click *Servers*, and then click *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, right-click on `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.
4. Type the maximum number of sessions to cache in the *Session Pool Size* text box of the *RESTful Web Service* area.
5. Type the session pool timeout value in the *Session Pool Timeout (minutes)* text box of the *RESTful Web Service* area.
6. Click *Save and Close*.
7. Right-click on the WACS server, for example, `MySIA.WebApplicationContainerServer`, and click *Restart Server*.

12.1.8.2.2.5 To enable HTTP basic authentication

HTTP basic authentication lets users make RESTful web service requests without providing a logon token. If HTTP basic authentication is enabled, users are prompted to provide their user name and password the first time they make a RESTful web service request.

> **Note**
>
> User names and passwords are not transmitted securely with HTTP basic authentication, unless it is used in conjunction with HTTPS.

When you enable HTTP basic authentication, you set the default HTTP basic authentication type to SAP, Enterprise, LDAP, or WinAD. Users can override the default HTTP basic authentication type when they log on.

Logging on to the BI platform using HTTP basic authentication consumes a license. If the session pool caching is used, the request uses the license associated with its cached session. If session pool caching is not used, a license is consumed while the request is in progress and released once the request is finished.

1. Log on to the Central Management Console (CMC) as an administrator.
2. Click *Server* > *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, right-click on `MySIA.WebApplicationContainerServer`, and click *Properties*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The *Properties* tab for the WACS server appears.

4. In the *RESTful Web Service* area, select *Enable HTTP Basic Authentication*.
5. (Optional) In the *Default Authentication Scheme for HTTP Basic* list, select the default type of HTTP basic authentication.
6. Click *Save and Close*.

When an end user logs on using HTTP basic authentication, they can specify the type of authentication to use. In a web browser, the user types `<authtype>\<username>` in the user name prompt, and `<password>` in the password prompt.

To log on using HTTP basic authentication programmatically, users add the `Authorization` attribute to the HTTP request header, and set the value to be `Basic <authtype>\<username>:<password>`.

Replace `<authtype>` with the authentication type, `<username>` with the user name, and `<password>` with the password. The authentication type, user name, and password must be base64-encoded as defined by RFC 2617. User names that contain the `:` character cannot be used with HTTP basic authentication.

Related Information

To configure session pool settings [page 428]

12.1.8.2.3 Cross-Origin Resource Sharing

12.1.8.2.3.1 To configure cross-origin resource sharing (CORS)

The *Cross-Origin Resource Sharing Configuration* (CORS) setting allows you to add a list of domain names to let users retrieve data from multiple sources on JavaScript-based web pages. This is necessary to get around the security policy that JavaScript and Ajax languages employ to prevent cross-domain access. To avoid compromising security, only those websites that may be accessed are added to the *Allow Origins* WACS server properties in CMC.

A *Max Age (minutes)* setting is also available to adjust the cache expiry time, which sets the maximum number of minutes that browsers can retain HTTP requests.

> **Note**
>
> By default, access to any and all domains are allowed with * (asterisk).

1. Log on to the Central Management Console as an administrator.
2. Click *Server* > *Servers List*.
3. Right-click on your Web Application Container Server (WACS); for example, right-click `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. In the *RESTful Web Service* area, go to the *Cross-Origin Resource Sharing Configuration* text box beside *Allow Origins:* and replace the * (asterisk) with your list of domain names, each separated by a comma. For example: `http://origin1.server:8080, http://origin2.server:8080`
5. In the *Max Age (minutes):* text box, type the maximum number of minutes that you want browsers to cache HTTP requests.
6. Click *Save and Close*.

12.1.8.2.4 Authentication

12.1.8.2.4.1 To configure web.xml to enable WinAD SSO

Configuring the RESTful web services to recognize Windows Active Directory Single Sign-On (WinAD SSO) requires edits to the `web.xml` configuration file, located on the BI platform server. For more information, see "Using the SDK > Authentication > To get a logon token using an Active Directory Single Sign-On (AD SSO) account" in the *Business Intelligence Platform RESTful Web Service Developer Guide*.

To have a client computer WinAD SSO login credentials recognized by the BI platform server, you must uncomment the `Kerberos Proxy filter` section of the `web.xml` and update values for `idm.realm`, `idm.princ` and `idm.keytab` that reflect the active directory environment used.

1. Locate the `web.xml` configuration at `<boe root>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. The following filepath is an example.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\java\
pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

2. In the `web.xml` file, uncomment the Kerberos Proxy Filter section by adding a comment close tag `-->` before the `<filter>` tag, and remove the closing comment tag `-->`

```
  <!-- Kerberos Proxy Filter
    - Uncomment this filter and the corresponding filter-mapping to enable
Kerberos SSO
    - for Windows AD (secWinAD) authentication.
    - The following options must be specified (the rest are optional):
    -   idm.realm
    -   idm.princ
    -   idm.keytab (unless using password, see below)
  -->

  <filter>
    <filter-name>WrappedResponseAuthFilter</filter-name>
      .
      .
      .
  </filter>

  <filter-mapping>
    <filter-name>WrappedResponseAuthFilter</filter-name>
    <url-pattern>/logon/adsso</url-pattern>
  </filter-mapping>

</web-app>
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Update the `<param-value>` for each setting of `idm.realm`, `idm.princ` and `idm.keytab` with those used in your active directory environment.

```
<init-param>
  <param-name>idm.realm</param-name>
  <param-value>ADDOM.COM</param-value>
  <description>
      Required: Set this value to the Kerberos realm to use.
  </description>
</init-param>

<init-param>
  <param-name>idm.princ</param-name>
  <param-value>BOE120SIAVMBOESRVR/bo.service.addom.com</param-value>

  <description>
      Set this value to the Kerberos service principal to use.
      This will be a name of the form HTTP/fully-qualified-host.
      For example, HTTP/example.vintela.com
      If not set, defaults to the server's hostname and the
      idm.realm  property above.
  </description>
</init-param>

<init-param>
  <param-name>idm.kdc</param-name>
  <param-value></param-value>
  <description>
      The KDC against which secondary credentials must be validated
      This can be used for BASIC fallback or credential delegation.
      By default the KDC will be discovered automatically and this
      parameter must only be used if automatic discovery fails, or
      if a different KDC to the one discovered must automatically be used.
  </description>
</init-param>

<init-param>
  <param-name>idm.keytab</param-name>
  <param-value>C:/winnt/BOE120SIAVMBOESRVR.keytab</param-value>
  <description>
      The file containing the keytab that Kerberos will use for
      user-to-service authentication. If unspecified, SSO will default
      to using an in-memory keytab with a password specified in the
      com.wedgetail.idm.sso.password environment variable.
  </description>
</init-param>
```

> **Note**
>
> The `idm.keytab` value refers to a filepath on the BI platform server. Values for `idm.realm` and `idm.prince` may be viewed from the Central Management Console. On the *Authentication* tab In the CMC, double-click *Windows AD*. The value for `idm.realm` is set with the *Default AD Domain* parameter, under *AD Configuration Summary*. The value for `idm.prince` is set with the *Service principal name* parameter, under *Authentication Options*.

4. Restart the WACS service so that the changes made to `web.xml` are recognized.
5. Use a client machien to verify that an AD SSO login token may be retrieved using the RESTful Web Services API, (for example, `http://<boe host>:6405/biprws/logon/adsso`).
6. Test the token by using a `GET` query including `X-SAP-LogonToken` in the header and using the `/infostore` API.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.8.2.4.2 To enable and configure trusted authentication

Trusted authentication is activated and configured through the Central Management Console (CMC) in areas that include *Authentication > Enterprise*, where Trusted Authentication is enabled and a shared secret key file is generated; *Users and Groups > User List*, where an account is created for a trusted user; and *Servers > Servers List > WACS > Properties*, where the *Retrieving Method* option is selected for `/logon/trusted` API logon token requests.

1. Log on to the Central Management Console as an administrator.
2. Go to *Authentication* > *Enterprise*, and then click *Trusted Authentication is enabled*.
3. Click *New Shared Secret*, and click *Download Shared Secret*.
4. Click *Save* and place the `TrustedPrincipal.conf` file in the default location, which is `<EnterpriseDir>\<platform>`.
   An example location appears as follows:

   ```
   "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI 4.0\win64_x64\"
   ```

   Note

   You can change the default location of the `TrustedPrincipal.conf` shared secret file by adding a command line entry in the CMC at *Servers > Servers List > WACS > Properties > Command Line Parameters*, and then restarting the WACS service. For example, a command line entry using `-Dbobj.trustedauth.home=` and the folder `SharedSecrets` placed at the root of the `C:\` drive of the BI platform server would appear as follows:

   ```
   "-Dbobj.trustedauth.home=C:\SharedSecrets"
   ```

   Note

   You can leave the option *Shared Secret Validity Period (days)* at the default value of zero (0) so that it does not expire. The *Trusted logon request is timeout after N millisecond(s) (0 means no limit)* option can be left at the default value of zero (0) so that there is no time limit for trusted logon requests.
5. Click *Update* to save the change.
6. Add a new user and password, for example `bob` and `Passw0rd`, in *Users and Groups* > *User List* using *Manage > New > New user*. Uncheck *User must change password at next logon*, then click *Create & Close*.

   Note

   You can also create a new user by clicking the *Create new user* icon, or by right-clicking in an open area of the window that lists user names, and select *New* > *New User*.
7. Go to *Servers* > *Core Services* > *WACS* > *Properties*, scroll down to the *Trusted Authentication Configuration* section and use the *Retrieving Method* menu to select either *HTTP_HEADER*, *QUERY_STRING* or *COOKIE*.

   Note

   You can optionally change the *User Name Parameter* from the default label of `X-SAP-TRUSTED-USER` to any other convenient label, (for example `UserName`, `bankteller`, or `nurse`) that RESTful web services developers must use.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8. Restart the service by right-clicking on the WACS server name, for example `MySIA.WebApplicationContainerServer`, and click *Restart Server*.

> **Note**
>
> Later changing the option under *Retrieving Method* as shown in step 7 does not require restarting WACS.

9. Verify that you are able to retrieve a logon token by using the `.../biprsw/logon/trusted/` API and sending a `GET` request with the default header label of `X-SAP-TRUSTED-USER` with the user name created in step 6.

12.1.8.2.4.3 To configure the command line parameter for relocating the `TrustedPrincipal.conf` shared secret configuration file

RESTful web services includes a command line parameter for choosing a different location for the trusted authentication `TrustedPrincipal.conf` file.

The `TrustedPrincipal.conf` file contains a shared secret key that is generated through the CMC: click *Authentication*, then double-click *Enterprise*. Select *Trusted Authentication is enabled* and then click the *New Shared Secret* button. Save the file by clicking *Download Shared Secret* and saving the file to the default location.

Update the Web Application Container Server (WACS) command line with a custom path for the `TrustedPrincipal.conf` file as follows:

1. Log on to the Central Management Console as an administrator user.
2. Click *Servers*, and then click *Servers List*.
3. Right-click on your WACS service, for example, `MySIA.WebApplicationContainerServer`, and click *Properties*.
   The *Properties* tab for the WACS server appears.
4. In the *Command Line Parameters* area, enter the path to the directory that will contain the `TrustedPrincipal.conf` file.

   The string is enclosed by double quotes as shown in the following example.

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

> **Note**
>
> The default location of the `TrustedPrincipal.conf` file is `<EnterpriseDir>\<platform>`. An example location is as follows:
>
> ```
> C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
> 4.0\win64_x64
> "
> ```

5. Click *Save and Close*.
6. Restart the service by right-clicking on the WACS server name, for example `MySIA.WebApplicationContainerServer` and click *Restart Server*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.9 WACS and your IT environment

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

12.1.9.1 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.

12.1.9.2 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. Then, 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 Information

Configuring HTTPS/SSL [page 412]

12.1.9.3 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.9.3.1 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*.

12.1.9.3.2 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.

12.1.9.4 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 BI platform servers in your deployment, see the "Understanding communication between SAP BI platform components " section of the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

Related Information

Understanding communication between BI platform components [page 165]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

12.1.9.5 To configure WACS on a multihomed machine

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

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

12.1.10 Configuring web application properties

The properties for web applications that are hosted on a WACS can be configured in the following ways:

- Properties that are often changed are exposed as configurable service properties for the WACS. To edit these properties, open the *Properties* page of the WACS in the Central Management Console (CMC), modify the value for the appropriate property, and click *Save*.
- To modify the session timeouts for web applications hosted on WACS, first determine whether the web application has any properties that can be configured in the CMC.
  If the web application has properties that can be modified in the CMC, then modify the `web_xml.ino` file for the web application. The file is **<WebAppName>**`_web_xml.ino`, where **<WebAppName>** is the name of the web application, and can be found in the **<EnterpriseDirectory>**`/java/pjs/services/`**<WebAppName>** directory.
  If the web application does not have properties that can be modified in the CMC, modify the `web.xml` file for the web application. This file can be found in the **<EnterpriseDirectory>**`/warfile/webapps/`**<WebAppName>**, where **<WebAppName>** is the name of the web application.
- To modify properties other than the session time out or the properties that appear on the *Properties* screen for the WACS in the CMC, modify the `.properties` file for the web application. For more information, see the "Managing applications through BOE.war properties" section of the *SAP BI platform Administrator Guide*.

> **Note**
>
> Do not modify the `web.xml`, `web_xml.ino`, or `.properties` files in the **<EnterpriseDirectory>**`/java/pjs/container/work/`**<ServerFriendlyName>** directory, as your change will be overwritten every time that the WACS starts or restarts.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> After you modify the properties for a WACS, you must always restart it.

Related Information

To change a server's properties [page 355]
The BOE war file [page 579]

12.1.11 Troubleshooting

12.1.11.1 To configure tracing on WACS

To configure tracing for WACS, see Logging traces for components [page 787]

12.1.11.2 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 Information

Web Application Container Server Metrics [page 913]

12.1.11.3 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 server state called “Started with Errors”. This state means that the WACS is running, but has one or more of these error conditions:

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

12.1.11.4 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 List of Running WACS Connectors and WACS Connector(s) Failed at Startup metrics. If the HTTP, HTTP through Proxy, or HTTP connectors do not appear in the List of Running WACS Connectors, these connectors are not able to start due to a port conflict.

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

12.1.11.4.1 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.

12.1.11.4.2 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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*.

12.1.11.5 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.

12.1.11.6 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*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. To start the WACS, right-click the server and click *Start Server*.

12.1.11.7 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.

12.1.11.8 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. In the *Web Application Container Service* section, clear the *Bind to All IP Addresses* check box.
4. In the *Bind to Hostname or IP Address* field, type `127.0.0.1`, and click *Save & Close*.
5. To start the WACS, right-click the server and click *Start Server*.
   The WACS that is configured this way accepts only connections from the local machine.

12.1.12 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”.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Core Services properties [page 869]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13 Backing Up and Restoring Your System

13.1 Overview of backup and restore

This chapter explains how to back up the BI platform and how to recover your system from hardware failure, software failure, and data loss. To execute a backup and recovery plan, you need an experienced SAP BusinessObjects Professional, System Administrator, and Database Administrator.

Related Information

Backing up the entire system [page 445]
Backing up BI content [page 451]
To back up server settings in the CCM on Windows [page 449]
To back up server settings on Unix [page 450]
Overview of system copying [page 462]

13.2 Terminology

Table 72:

Term	Definition
Data replication	Data replication is the process of creating one or more copies of your data. The copies are updated in real time; for example, when using mirrored drives. It offers real time data protection from physical data damage, but because the drives are constantly being updated it is not possible to revert your system to an earlier state if data becomes corrupted or accidentally removed.
Versioning	Versioning creates multiple versions of a specific file or files on your system. In this case, it is possible to revert your system to an earlier state. All data versions are typically stored on the same host system. If this system is compromised or damaged, you risk losing both the current version and the older versions. Similarly, Undelete functions keep copies of "deleted" files for later recovery, but again these are usually stored on the same host system as the original data. It doesn't offer protection from physical data damage (for example, disc failure).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Term	Definition
Bare-metal system backup	A bare-metal system backup is a backup of an entire file system, including the operating system. A bare-metal system backup is intended to be used to restore a backed-up system to hardware that contains no software or operating system. For bare-metal system backups, in case of failure, the entire file system (including the OS) is restored to identical hardware, or, if your restore tools support hardware-independent restore, to any hardware.
Bare-metal system backup vs. application backup	A bare-metal system backup creates a copy of the entire system, including the operating system. A bare-metal system backup allows you to revert to an earlier version of the system as a whole. An application backup backs up files related to individual applications. The BI platform supports bare-metal system backups but not application backups. For bare-metal system backups, in case of failure, the entire file system (including the OS) is restored to identical hardware, or, if your restore tools support hardware-independent restore, to any hardware. A complete BI platform system backup is called a backup set.
Backup set	A backup set comprises these individual backups, created at the same time: • A backup of the CMS system database • A bare-metal backup of the entire file system, including the operating system, of all machines in the BI platform deployment • A backup of the Input FRS and the Output FRS file stores (if not included in the BI platform file system) • A backup of the web tier components (if not included as part of the BI platform file system) • A backup of the auditing database
Cold vs. hot backup	A cold backup is performed while the system is stopped and unavailable to users. A hot backup is performed while the system is running and available to users, and data can change while the backup is being performed. Also, when performing a hot backup, you must perform the backup steps in order, which is not the case with a cold backup. The BI platform supports both cold and hot backups. Hot backup is sometimes called “online backup”.

13.3 Use cases for backup and restore

The following table describes the goals you might want to achieve given the resources you might have, and directs you to the most appropriate backup solution.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Goal	Resources required	Solution
Goal: Restore a system 1. My BI platform system was corrupted. Therefore, I need to restore it to the working state it was in when it was last backed up. 2. A machine hosting the BI platform was damaged. I need to replace it with a new machine.	• A target system with identical hardware to the source system AND • Backups of the source system	Use the system backup and restore workflow detailed in this guide. See the Backing up the entire system [page 445] procedure. Recreate the target system from backups of the source system.
Goal: Restore objects I want to recover a document or other object that was accidentally deleted.	• Backups of the source system databases and files AND • Detailed system information described in To export from a source system [page 466]	Using backups, build a copy of the system on another machine, using the System Copy workflow in the "Copying your BI platform deployment" chapter. Then, use the promotion management tools to promote the accidentally deleted objects from that new system. See the System Copy workflow, starting with Planning to copy your system [page 463], and follow the instructions for the rest of the chapter. **Note** You can create your target system on a computer with an existing BI platform deployment of the same release, support package, and patch level, or a "clean" computer with no BI platform installed.
Goal: Restore objects 2 I want to recover a document or other object that was accidentally deleted.	A system where promotion management versioning is in use	Use the promotion management application to recover an earlier version of the document. For details, see the related topic on promotion management.
Goal: Back up objects I want to back up a small number of objects (for example: documents, folders, users).	A system where promotion management versioning is in use	Use the promotion management application to back up BI content and then export the content to Business Intelligence Archive (LCMBIAR) files. If content is corrupt or missing, you can restore it later, without restoring the entire system. For details, see the related topic on promotion management.

Related Information

Backups [page 445]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Planning to copy your system [page 463]
Overview [page 473]

13.4 Backups

A backup and recovery plan consists of steps to take in the event of a system failure due to a natural disaster or unexpected failure. The plan aims to minimize the effects of the disaster on daily operations so that you can maintain or quickly resume critical functions.

When backing up your BI platform deployment, you have three options:

- Backing up the entire system, which allows you to restore the entire system. In this case, restoring only a portion of the system is not possible. If you want to rebuild the BI platform instead of restoring it from a backup, see the related topic describing system copying.
- Backing up server settings, which allows you to restore only server settings without restoring other objects, preserving the current state of your system's BI content.
- Backing up BI content (for example, documents), which allows you to selectively restore parts of BI content without the need to restore all objects.

See the related topics for details on all three types of backups.

> **Tip**
>
> To avoid data loss, regularly perform backups.

> **Tip**
>
> You can back up a BI platform system and then restore it to the same or a different host computer to create a copy of the system.

Related Information

Backing up the entire system [page 445]
Backing up server settings [page 448]
Backing up BI content [page 451]
Overview of system copying [page 462]

13.4.1 Backing up the entire system

Back up your entire BI platform system by performing a cold or hot backup, which creates a backup set. Keeping multiple backup sets from different times gives you more options when restoring the system. Back up your system as frequently as your organization's business needs require.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

You can choose to stop your BI platform system and perform a cold backup, or you can perform a hot backup. With a hot backup, the system stays live and available to users during the backup process. It has the advantage of no downtime for your system.

> **Note**
>
> We recommend writing the transaction log to a file system other than the main database server system, regularly backing up this transaction log, and keeping it with the other files in the backup set.

> **Note**
>
> If you back up auditing data, make sure to include the database transaction log for the auditing database with your backup file set. You do not need to include the auditing temporary files with the backup.

13.4.1.1 Hot backups

The hot backup feature allows you to back up your BI platform system while continuing to allow users to use the system normally. If your business must continue operating while your system is backing up, enable and configure hot backups in the Central Management Console.

The *Hot Backup Maximum Duration* setting specifies the maximum amount of time that you expect the backup to take—from the time when the CMS backup begins to the time when the FRS backup ends. If the duration you specify is too short, files may be deleted before the backup has a chance to copy them. To avoid this, it is safer to overestimate the time required. Balance this concern against system resources because a high value may slightly increase your FRS file store size.

> **Note**
>
> Hot backup is enabled as long as the *Enable Hot Backup* check box is selected in the CMC; the *Hot Backup Maximum Duration* setting does not affect whether or not hot backup is enabled.

It is easiest to restore your system to a specific backup time. For example, if your system backups are performed daily at 3:00 AM, you can easily restore the system to the state it was in when the CMS system backup started (3:00 AM on the date of your choice). After a CMS database or auditing database failure, if you have enabled transaction logging on the CMS database or the auditing database, you can restore the system to the state it was in immediately before the failure.

For maximum safety, save transaction logging records at a different location than your primary database backup records. This ensures that, in the case of database failure, you can restore the database to the state it was in prior to failure.

> **Note**
>
> Due to a limitation on transaction log size on older versions of IBM DB2, hot backup and transaction-log-related tasks are supported only if the CMS system database is hosted on DB2 database server version 9.5 Fix Pack 5 or newer (for the 9.5 line), and 9.7 Fix Pack 1 or newer (for the 9.7 line).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> We recommend writing the transaction log to a file system other than the main database server system, regularly backing up this transaction log, and keeping it with other files in the backup set.

Crystal Reports 2013 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.

13.4.1.1.1 To enable hot backups

1. Open the Central Management Console (CMC).
2. From the *Manage* area, open the *Settings* page.
3. In the *Hot Backup* section, select *Enable Hot Backup*.
4. Enter the maximum number of minutes you expect the backup to take under *Hot Backup Maximum Duration (Minutes)*.

   Be sure to include the time required to back up both the CMS database and the file system of the BI platform host machine.

   > **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.

   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 related link regarding hot backups.
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.

Related Information

Hot backups [page 446]
To perform a hot or cold system backup [page 448]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13.4.1.2 To perform a hot or cold system backup

If you want to perform a hot backup, first see the related topic about hot backups for prerequisites and more information. If you are performing a cold backup, stop all nodes in your BI platform deployment.

> **Caution**
>
> If you perform a backup without enabling hot backup and without stopping all nodes, data inconsistencies may result between the CMS database and the FRS file store.

> **Note**
>
> For hot backups, it is important that the procedures are started in the sequence described. For cold backups, the procedures can be performed in any order. In either case, it is not necessary to wait for each backup step to complete before starting the next step.

1. Use your database vendor tools to back up the Central Management Server (CMS) system database.

   > **Note**
   >
   > For hot backups, use the database vendor's backup tools in online atomic mode.

2. Use your database vendor tools in online atomic mode to back up the BI platform auditing database.
3. Back up the entire file system, including the operating system, of all machines in the BI platform deployment.
   a. If the Input and Output FRS file stores are not included in the BI platform backup (separate host machines), create a backup copy of both using your file-backup tools.
   b. If the web-tier components are not included in the BI platform backup (separate host machines), create a backup copy of them using your file backup tools.

   For hot backups, use atomic file backup tools if possible.

If you performed a cold backup, wait for all backups to complete and then start your BI platform nodes.

Related Information

Hot backups [page 446]

13.4.2 Backing up server settings

In order to protect your system from misconfigured server settings, back up your server settings to a BIAR file on a regular basis. Having available backups of your servers allows you to restore settings without having to restore your Central Management Server (CMS) system database, File Repositories, or Business Intelligence content.

It is essential that you back up your server settings whenever you make any changes to your system's deployment. This includes creating, renaming, moving, and deleting nodes, and creating or deleting servers. It is recommended that you back up your server settings before you change any of the settings, and then again after you're satisfied with the changes that you've made.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Use the Central Configuration Manager (CCM) or a script to back up your BI platform server settings to a BIAR file, and then store the file on a separate machine or storage media.

> **Note**
>
> If you are backing up or restoring server settings in a deployment where SSL is enabled, you must first disable SSL through the CCM, and then re-enable it when the backup or restore is complete.

On Windows, the `BackupCluster.bat` script is located in the **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` directory.

On Unix, the `backupcluster.sh` script is located in the `/`**<INSTALLDIR>**`/sap_bobj/enterprise_xi40/`**<platform64>**`/scripts` directory.

13.4.2.1 To back up server settings in the CCM on Windows

This procedure backs up the server settings for an entire cluster. It is not possible to back up the settings for individual servers.

> **Note**
>
> If you are using a temporary CMS, you must use the CCM on a machine that has a local CMS binaries installed.

1. Start the CCM, and on the toolbar, click *Back up Server Configuration*.
   The *Server Configuration Backup Wizard* appears.
2. Click *Next* to start the wizard.
3. Specify whether to use an existing CMS to back up server configuration settings or to create a temporary CMS.
   - To back up server settings from a system that is running, select *Use existing running CMS*, and click *Next*.
   - To back up server settings from a system that is not running, select *Start a new temporary CMS*, and click *Next*.
4. If you are using a temporary CMS, select a port number for the CMS to run on, and specify the database connection information.

   To minimize the risk of users accessing your system while you are restoring your system, specify a port number that is different than the port numbers that your existing CMS uses.
5. Enter the cluster key, and click *Next* to continue.
6. When prompted, log on to the CMS by specifying the system and user name and password of an account with administrative privileges, and click *Next* to continue.
7. Specify the location and name of a BIAR file that you want to back up the server configuration settings to, and click *Next* to continue.
   The *Confirmation* page displays the information that you have provided.
8. Verify that the information displayed on the *Confirmation* page is correct, and click *Finish* to continue.
   The CCM backs up the server configuration settings for the entire cluster to the BIAR file that you specify. Details of the backup procedure are written to a log file. The name and path of the log file are displayed in a dialog box.
9. If the backup operation failed, check the log file to determine the reason.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

10. Click *OK* to close the wizard.

13.4.2.2 To back up server settings on Unix

On Unix, use the `serverconfig.sh` script to back up your deployment's server settings to a BIAR file.

1. Select *5 - Back up server configuration* and press `Enter`.
2. Specify whether to use an existing CMS to back up server configuration settings or to create a temporary CMS.
   - To back up server settings from a system that is running, select *existing*, and press `Enter`.
   - To either back up server settings from a system that isn't running, or to restore server settings, select *temporary*, and press `Enter`.
3. If you are using a temporary CMS to back up your server settings, on the next several screens, select a port number for the temporary CMS to run on, and the connection information to the CMS system database.

   To minimize the risk of users accessing your system while you are restoring your system, specify a port number that is different than the port numbers that your existing CMS uses.
4. When prompted, log on to the CMS by specifying the system and user name and password of an account with administrative privileges, and press `Enter`.
5. When prompted, specify the location and name of a BIAR file that you want to back up the server configuration settings to, and press `Enter`.
   A summary page displays the information that you have provided.
6. Verify that the information displayed is correct, and press `Enter` to continue.
   The `serverconfig.sh` script backs up the server configuration settings for the entire cluster to the BIAR file that you specify. Details of the backup procedure are written to a log file. The name and path of the log file are displayed.
7. If the backup operation failed, check the log file to determine the reason.

13.4.2.3 To back up server settings with a script

You can back up the server settings in your deployment by running the `BackupCluster.bat` file on Windows or the `backupcluster.sh` script on Unix.

On Windows, the `BackupCluster.bat` file is located in the **`<INSTALLDIR>`**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` directory.

On Unix, `backupcluster.sh` is located in the `/`**`<INSTALLDIR>`**`/sap_bobj/enterprise_xi40/`**`<platform64>`**`/scripts` directory.

Related Information

BackupCluster and RestoreCluster scripts [page 459]

 © 2015 SAP SE or an SAP affiliate company. All rights reserved.

13.4.3 Backing up BI content

It is recommended that you use the promotion management application to regularly back up your Business Intelligence content, such as reports, users and groups, and universes. Having current backups of your content makes it possible to restore your Business Intelligence without having to restore your entire system or your server settings.

For more information about using the promotion management tool, see the “Promotion Management” chapter.

If you are using Subversion with the promotion management tool, see the “Version Management” chapter.

13.5 Restoring your system

If your system is damaged or corrupted, you can restore the entire system, which restores the BI platform. Depending on the condition of your system, a complete restoration may not be required. If the system is working normally but you have lost or corrupted content, you can choose to restore only Business Intelligence (BI) content. If BI content is valid but your platform servers have become misconfigured, you can restore only server settings.

The procedure is the same for restoring from a hot or cold backup.

Related Information

Restoring your entire system [page 451]
Restoring server settings [page 456]
Restoring BI content [page 458]

13.5.1 Restoring your entire system

When you restore the entire system, the BI platform cluster is also restored. Depending on what failed in the system, you may still have the option to do only a partial restore.

If any of the following components fails or is lost, you must restore your entire system:

- The CMS database

  > **Note**
  >
  > If the rest of the BI platform operates normally but the CMS database has crashed, you can restore the CMS database, without restoring the entire system.

- The FRS file store
- The machine's file system

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> For a full system restore, the target system does not require the BI platform to be already installed.

If only the auditing database is corrupted or lost, you can restore the auditing database, without restoring the entire system.

If your web-tier content is corrupted or lost, you can restore the web-tier content, without restoring the entire system.

Related Information

To restore your entire system [page 452]
To restore only the auditing database [page 453]
To restore web-tier content [page 454]
To restore only the CMS database [page 454]

13.5.1.1 To restore your entire system

Before restoring your system, you must use the Central Configuration Manager (CCM) to stop all nodes in your BI platform deployment, and you must choose the point in time when you want to restore the system to.

> **Note**
>
> If you may want to restore the system to its current state, back up the system before restoring it.

1. Locate the following backup files:
   - CMS database backup
   - Input FRS and Output FRS file store backups
   - Backups of file systems for every host machine in the BI platform cluster

   > **Note**
   >
   > Make sure to validate the backups, and ensure that all of the files listed above are from the same backup set. If the backup set was obtained as a hot backup, ensure that the CMS database backup start timestamp is earlier than the matching FRS file store, web tier, and host-machine file-system timestamp. All these files will be required, even if only one component failed.
2. Use your file restore tools to restore the file system of all host machines in the BI platform cluster.
3. Use your file restore tools to restore the Input and Output FRS file stores.
4. Use your database tools to restore the CMS database.
5. If you have changed the CMS database password since the backup was created, use the CCM to update the CMS database password on all nodes and BI platform host machines.
6. If you use the Auditing feature:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

a. Locate the latest backups and transaction logs for the auditing database.
b. Use the database tools to restore the auditing database.
c. Perform a roll forward on the auditing database, replaying the transaction log.

7. Choose one of the following options for restoring your search index:
   - If you want to run the search index recovery script, see To run the search index recovery script [page 455] and follow the instructions there. This will provide you with a full index more quickly.
   - If you want to rebuild your search index rather than use the recovery script, use the CCM to restart your BI platform nodes. This is a simpler procedure, but while the index is rebuilding you will have only partial search access to the platform data.
8. Start the system, and note the time for use during the post-requisite steps.
9. Verify that your system is working as expected, and perform a sanity test.

Once the system has been verified, take the following actions:

- Run the Repository Diagnostic Tool to remove any unused temporary files and check repository consistency. See the Repository Diagnostic Tool section of this guide.
- If you did not use the index recovery script, rebuild your platform search index.
- Any publishing jobs in process at the time the system was backed up will display as failed. Do not rerun these instances; start new publishing jobs.
- If your auditing database was restored, then you must run an SQL query to remove any events that fall between the database failure and the restart time (the time you noted in step 8). For example: `delete from [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

Related Information

Indexing Content in the CMS Repository [page 676]

13.5.1.2 To restore only the auditing database

Before restoring your auditing database, use the Central Configuration Manager (CCM) to stop all nodes in your BI platform deployment. You must also choose which point in time you want to restore the database to.

> **Note**
>
> Perform this task only if you are sure the auditing database is the only compromised component of the BI platform. If additional components are affected, you must perform a full system restore.

1. Locate the latest backups and transaction logs for the auditing database.
2. Use the database tools to restore the auditing database.
3. Perform a roll forward on the auditing database, replaying the transaction log.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To restore your entire system [page 452]

13.5.1.3 To restore web-tier content

Before you restore your web-tier content, you must stop all nodes in your BI platform deployment using the Central Configuration Manager (CCM). You will also need to decide which point in time you want to restore the web-tier content to.

If you want to have the option to return to the current state of the system, you must perform a backup of the system before restoring.

If the web-tier is corrupted it can be restored individually.

1. Use file restoration tools to restore the web tier folders on the web-tier host-machine.
2. Use the CCM to restart all nodes for your BI platform deployment.

13.5.1.4 To restore only the CMS database

> **Note**
>
> Perform this procedure if only the CMS database has crashed. If the database is corrupted or other components have been compromised you must perform a full system restore.

Repair or replace the CMS database host-machine. If replaced, ensure that it has the same system name as the previous host-machine, as well as the same port settings and database credentials.

> **Note**
>
> If it is not possible to restore the machine using the same name and credentials, you will need to use the CCM to update this database connection information for each node in the cluster and restart those nodes.

1. Stop all BI platform nodes using the CCM.
2. Locate the latest CMS database backup set.
3. Using your database tools, restore the CMS database.
4. Locate the most recent CMS database transaction log—that is, the log that contains transactions performed after the last backup.
5. Replay the entire transaction log for the CMS database.
6. Use the CCM to start the BI platform nodes.

Once you have verified the system is working properly, take the following actions:

- Run the Repository Diagnostic Tool to remove any unused temporary files and check repository consistency. See the Repository Diagnostic Tool section of this guide.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Any publishing jobs in process at the time the system was backed up will display as failed. Do not rerun these instances; start new publishing jobs.

Related Information

Indexing Content in the CMS Repository [page 676]

13.5.1.5 The search index recovery

The platform search feature maintains a series of index and information files across your system to help it search more efficiently. If it is necessary to restore the system, these information files may develop inconsistencies. You can repair these inconsistencies by either using the index recovery script or rebuilding the index.

Rebuilding the index is a straightforward procedure, but the process will consume significant resources and take some time to complete, and searches conducted during the rebuild will only return results for the indexed portions of the database. The recovery script involves a more complicated procedure, but will provide you with a full, working index more quickly.

If you are restoring a deployment with multiple computers, run the script on any computers hosting the search service. For the first computer in a cluster, use the `-Both` option, then on all subsequent computers in that cluster, use the `-ContentStore` option.

Related Information

Indexing Content in the CMS Repository [page 676]

13.5.1.5.1 To run the search index recovery script

- Confirm that the CMS is running, and stop all Adaptive Processing Servers (APS) with the Search Service installed.

  > **Note**
  >
  > You must stop these APSs as quickly as you can after the node starts.

- Set `JAVA_HOME` to the `sapjvm/bin` location in the BI platform installation directory.
- The Platform Search data directory is accessible from the machine where you are running the script.

1. On the CMS or APS host-machine, open a command-line window (if using a Windows OS).
2. Switch to the following directory **<INSTALLDIR>**`\SAP BuinsessObjects Enterprise XI 4.0\java \lib\`.

   Unix machines use the equivalent Unix file path.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Type `java -jar platformSearchOnlineHotbackupRestore.jar` and press *Enter*.
4. When prompted, enter the following information and press *Enter*:
   - Your BI platform installation location (for example, **<INSTALLDIR>**`/SAP businessObjects Enterprise XI 4.0`)
   - Your CMS logon credentials, including the CMS name, user ID and password, and authentication type. Authentication type has the following options:
     - `secEnterprise`
     - `secLDAP`
     - `secWinAD`
     - `secSAPR3`
5. When you are prompted for the index restore type, type one of the following options and press *Enter*.

Value	Description
`-Both`	This should be used for single server deployments, or, in multi-machine deployments, for the first APS host-machine with the search service: On a system with multiple search APSs, the first time the script is run, use the `-Both` value (updates the database and content store). When the script is run for all other search APSs, use the `-ContentStore` value (updates only the content store).
`-ContentStore`	This should be used when running the script on APS host-machines with the search service installed, unless it is the first computer in the cluster where the script is run.
`-Exit`	Exit the script without performing an index restore.

6. When the script has finished running, close the command-line window (for Windows machines).

Start all stopped APSs.

13.5.2 Restoring server settings

If you need to restore your system's server settings from a BIAR file, you can use either the Central Configuration Manager (CCM) or the RestoreCluster script to restore the server settings. Restoring server content from a BIAR file doesn't affect Business Intelligence content such as reports, users and groups, or security settings.

> **Note**
>
> When restoring server settings, only the restoration of the settings for an entire cluster is supported. It is not possible to restore the settings for only some of the servers in the cluster.

> **Note**
>
> If you are backing up or restoring server settings in a deployment where SSL is enabled, you must first disable SSL through the CCM, and then re-enable it when the backup or restore is complete.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13.5.2.1 To restore server settings with the CCM on Windows

You can use the Central Configuration Manager (CCM) to restore server settings. After you restore server settings, you must recreate your system's nodes on every computer in your system's cluster.

1. Stop all the nodes on all of the computers in the cluster for which you are restoring server configuration settings by stopping the Server Intelligence Agent for each node.
2. Start the CCM on a computer that has a CMS.
3. From the toolbar, click *Restore Server Configuration*.
   The *Restore Server Configuration Wizard* appears.
4. Click *Next* to start the wizard.
5. When prompted, provide the port number for the temporary Central Management Server (CMS) to use, and the information to connect to the CMS system database, and click *Next* to continue.
6. Enter the cluster key, and click *Next* to continue.
7. When prompted, log on to the CMS by entering the CMS name and the user name and password of an account with administrative privileges, and click *Next* to continue.
8. Specify the location and name of the BIAR file that contains the server configuration settings you want to restore, and click *Next* to continue.
   A summary page displays the contents of the BIAR file.
9. Click *Next* to continue.
   A summary page displays the information you entered.
10. Click *Finish* to continue.
    A warning message indicates that existing server settings will be overwritten by values in the BIAR file, and if you proceed, the current server settings will be lost.
11. Click *Yes* to restore the server configuration settings.

    The CCM restores the server configuration settings for the entire cluster from the BIAR file. Details of the restoration are written to a log file. The name and path of the log file appear in a dialog box.
12. If the restore operation failed, check the log file to determine the reason.
13. Click *OK* to close the wizard.

The server settings from the BIAR file are restored on your system. Any nodes and servers existing in the BIAR file that did not exist on the system prior to the restore are created.

> **Note**
>
> Nodes and servers that existed on the system, but not in the BIAR file, are removed from the repository. The nodes and servers still appear in the CCM, but you can manually delete the `dbinfo` and `bootstrap` files for a node.

You must recreate the nodes in your system on each computer in the cluster.

Related Information

Using nodes [page 366]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13.5.2.2 To restore server settings with the CCM on Unix

On Unix machines, use the `serverconfig.sh` script to restore your deployment's server settings from a BIAR file.

1. Select *6 - Restore server configuration*, and press `Enter`.
2. Enter a port number for the temporary Central Management Server (CMS) to use, and press `Enter`.
3. On the next screens, specify the connection information to the CMS system database.
4. When prompted, log on to the CMS by specifying the system and user name and password of an account with administrative privileges, and press `Enter`.
5. When prompted, specify the location and name of a BIAR file that you want to restore the server configuration settings from, and press `Enter`.
   A summary screen displays the information that you have provided.
6. Verify that the information displayed on the screen is correct, and press *Enter* to continue.
   The `serverconfig.sh` script restores the server configuration settings for the entire cluster from the BIAR file that you specify. Details of the restore procedure are written to a log file. The name and path of the log file are displayed on the screen.
7. If the restore operation failed, check the log file to determine the reason.

13.5.2.3 To restore server settings with a script

If you prefer, you can restore the server settings of your deployment by running the `RestoreCluster.bat` script on Windows, or the `restorecluster.sh` script on Unix.

On Windows, `RestoreCluster.bat` is located in the **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` directory.

On Unix, `restorecluster.sh` is located in the `/`**<INSTALLDIR>**`/sap_bobj/enterprise_xi40/`**<PLATFORM64>**`/scripts` directory.

Related Information

BackupCluster and RestoreCluster scripts [page 459]

13.5.3 Restoring BI content

If you've backed up Business Intelligence (BI) content to LCMBIAR files, you can use the promotion management tool to restore BI content, without restoring your entire system. For more information, see the “Promotion Management” chapter.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13.6 BackupCluster and RestoreCluster scripts

The following table describes the command-line parameters used with the `BackupCluster` script.

> **Note**
>
> This script only backs up server settings for a cluster. Other data must be backed up separately.

Table 73: BackupCluster parameters

Name	Description	Example
`-backup`	The name and path of the BIAR file that you want to back up your system's server settings to restore.	`-backup "C:\Users\Administrator\Desktop\my.biar"`
`-cms`	The host name of the machine where your system's Central Management Server is located. If your CMS is running on any other port than the default port, 6400, you must also specify the port number.	`-cms mycms:6400`
`-username`	The user name of an Administrator account.	`-username Administrator`
`-password`	The password of an Administrator account.	`-password Password1`

The following table describes the command-line parameters used with the `RestoreCluster` script.

Table 74: RestoreCluster parameters

Name	Description	Example
`-restore`	The name and path of the BIAR file that contains the server configuration settings that you want to restore.	`-restore "C:\Users\Administrator\Desktop\my.biar"`
`-username`	The user name of an Administrator account.	`-username Administrator`
`-password`	The password of an Administrator account.	`-password Password1`
`-displaycontents`	Displays a list of nodes and servers that the BIAR file contains.	`-displaycontents "C:\Users\Administrator\Desktop\my.biar"`

> **Note**
>
> Run the `RestoreCluster` script with the `-displaycontents` parameter to display the contents of the BIAR file before you restore the server settings.

The following parameters are required if you are backing up server settings from a system that is not running, or if you are restoring server settings.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 75: Parameters used when using a temporary CMS

Name	Description	Example
-usetempcms	Creates a temporary CMS for the specified operation. After the operation is complete, the temporary CMS is stopped.	**-usetempcms**
-cmsport	The port number of the temporary CMS.	**-cmsport 6700**
-dbdriver	The database driver of the CMS system database. Accepted values are: • **db2databasesubsystem** • **maxdbdatabasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqlserverdatabasesubsystem** • **sybasedatabasesubsystem** • **sqlanywheredatabasesubsystem** • **newdbdatabasesubsystem** Note The **newdbdatabasesubsystem** parameter is for use with SAP HANA databases.	**-dbdriver sqlserverdatabasesubsystem**
-connect	The CMS system database connection string.	**-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"**
-dbkey	The cluster key.	**-dbkey abc1234**

Example

The following example shows how to back up your server settings to a BIAR file, using an existing CMS.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

Example

The following example shows how to display the contents of a BIAR file.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Example

The following example shows how to restore your settings from a BIAR file. You must always use a temporary CMS when restoring server settings.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

14 Copying Your BI Platform Deployment

14.1 Overview of system copying

This chapter describes how to create a duplicate of your BI platform deployment for testing, standby or other purposes.

Related Information

Overview of backup and restore [page 442]

14.2 Terminology

Term	Definition
Source System	The original BI platform deployment.
Target System	The new deployment you want to create.
System Copy	The act of creating a duplicate of an existing BI platform deployment.
Homogeneous System Copy	The act of creating a duplicate system where the source and target systems have the same type of operating system and database. The BI platform supports only homogeneous system copying.
Heterogeneous System Copy	The act of creating a duplicate system where the source and target systems use different types of operating systems or databases but are based on the same data.
Database Copy	The act of creating a duplicate of the CMS system or auditing database using database vendor tools.

14.3 Use cases for system copying

The following table describes the goals you might want to achieve given the resources you might have, and directs you to the most appropriate solution.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Goal	Resources required	Solution
Goal: Identical copy I want to create a duplicate system for standby or testing with an identical hardware configuration and IP addresses/machine names.	• A target system with identical hardware to the source system AND • Backups of the source system or access to the source system to make a backup from.	Use the system backup and restore workflow detailed in this guide. See the Backing up the entire system [page 445] procedure. Recreate the target system from backups of the source system.
Goal: Copy I want to create a duplicate system for standby, testing, or training that has different hardware and IP addresses/ machine names from the source system.	• Source System (running or stopped) OR Backups of source system databases and files. AND • Detailed system information described in To export from a source system [page 466]	Use the System Copy workflow, starting with Planning to copy your system [page 463], and follow the instructions for the rest of the chapter. **Note** You can create your target system on a computer with an existing BI platform deployment of the same release, support package, and patch level, or a clean computer with no BI platform installed.

Related Information

Backups [page 445]
Planning to copy your system [page 463]

14.4 Planning to copy your system

A system copy does not have to reflect your current system. You can create a copy of your system and wait some time before proceeding to recreate the copy on the target system, or you can use a previous backup of the source system as the base for your target system. This will mean that the copy will be of the system as it was at the time the copy was created. For example, if you wait one month, the copy will recreate the system as it was one month ago.

After reviewing the use cases in the preceding section and deciding which one best suits your needs, you should develop a system copy plan.

Create a system copy plan

When planning to copy a system, you should decide the following in advance:

- Will the source system will be stopped or active while the copy is being made? (The procedure can be done under either circumstance.)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

    - If the source system is stopped, how much downtime will be required?
    - Plan some time for testing to ensure the integrity of the target system.
- Which database tools you want to use for database backup and restoration.
- Which machines the target system will be deployed on, and where each node will be hosted.
- Which optional components you want to copy.
- The database type to use for the target CMS database, and any other optional databases you will be copying.

You should also give consideration to the following:

- Which BI platform components your source system has installed. You can use the *Add/Remove > Modify* function of the installation program to view the list of currently installed components.
- If the target system is installed on a different hardware setup from the source system, may need to tune the target system for better performance. See the information about improving your system performance in the *SAP BusinessObjects Business Intelligence sizing companion guide*.
- You may want the target system to report from reporting databases other than the source system databases. In this case you will need to change the database connection information for the reporting databases. You can do this by keeping the same DSN name but pointing to DSN on the target system to another database.

Required source system components

- CMS system database
- FRS file store
- Semantic layer configuration files
- Auditing database (optional)
- Monitoring database (optional)
- Promotion management Subversion database (optional)

14.5 Considerations and limitations

You should be aware of the following considerations when making a copy of your BI platform deployment.

Area	Consideration
SAP Business Warehouse integrations	If you are using the BI platform and SAP ERP or BW in an integrated environment, before copying your system, read the SAP system copy documentation. The system copy guides are available at http://www.sdn.sap.com/irj/sdn/systemcopy (SMP login required). Choose your SAP NetWeaver version; the relevant copy guides can be found in the installation guides folder.
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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Area	Consideration
Installation path	The installation path on the source and target locations must be identical: for example, if you installed the source system to `C:\SAP BusinessObjects Enterprise XI 4.0`, you must install the target to `C:\SAP BusinessObjects Enterprise XI 4.0`.
Host operating system	The source and target operating systems must be the same.
CMS database software type	CMS source and target databases must be of the same type. You will have the option of changing to another supported database type after copying the system.
Auditing database software type	If you are copying auditing data, the auditing source and target databases must be of the same type. After the copy has been created, you can establish a new database of a different type. **Note** If you establish a new database, existing events will not be copied to that database, only new events will be recorded to the new database.
Web tier customization	The copy procedure will not copy web tier components from the source system. If you customized the web tier (modified `.properties` files in the `custom` folder, for example) you must manually apply those customizations to the target.
Topics not covered by these instructions	This workflow does not describe how to export or import a database. Use your database vendor tools for database copying and restoring.

The following data will be copied during the system copy procedure:

- The CMS repository database. (contains reports, analytics, folders, rights, users and user groups, server settings, and other BI content and system content)
- The Auditing database. (contains auditing events triggered by BI platform servers or client applications)
- The Monitoring database. (contains trending data from metrics, probes, and watches)
- The Promotion Management database. (contains different versions of reports, analytics, other BI resources, and version information)

  Note

  For a description of the databases and their contents, see the Databases [page 34] section of this guide.
- Semantic layer configuration files

Web tier configuration, search index, and any data not specifically mentioned above are not copied.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Considerations for file recovery copies

If you are copying a system for the specific purpose of recovering a file that was accidentally deleted, you should be aware of the following additional considerations:

Using your backup, perform the steps in the procedure To import to a target system [page 470] on the production system.

- Do not install all nodes, just install the first node which will contain the CMS and its database.
- Do not install auditing, Promotion Management, or monitoring databases.
- Do not recreate connections to the auditing or reporting databases.

Use LCM to promote the object you want to recover from the target system to the source system.

14.6 System copy procedure

The following procedures guide you through the two stages of copying your BI platform deployment.

14.6.1 To export from a source system

You will need to make note of the following information from the source system. If you want to write this information down there is a worksheet you can use at System copy worksheet [page 940].

Property	Location
The CMS cluster key (make sure to keep the record secure).	Created by the system administrator when the BI platform was installed.
The name of the nodes.	Go to the *Servers* tab of the CMC, on the left tree expand *Nodes*.
The machine name and the BI platform installation folder for each machine in the deployment.	Go to the *Servers* tab of the CMC, right-click the CMS and select *Placeholders*. Look for the value of the `%INSTALLROOTDIR%` placeholder.
The BI platform administrator password (make sure to keep the record secure).	Created by the system administrator when the BI platform was installed.
All database connections that might be used by the CMS, and the user names and passwords associated with those connections. This can include auditing database if you want to copy this information. Make sure to get this information for all machines in the cluster.	Go to the *Servers* tab of the CMC, right-click the CMS and select *Metrics*. Look for the following metrics: • *System Database Connection Name* • *System Database Server Name* • *System Database User Name*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Location
Note If you are copying the auditing database, you also need the auditing database connection names and credentials.	• *Data Source Name* • *Auditing Database Connection Name* (optional) • *Auditing Database User Name* (optional)
For every machine in the cluster, the details (client types, versions) of any other database connections (used by universes and reports for example). Make sure to include user names and passwords.	For Crystal reports that report directly from databases, look at the connection information using the SAP Crystal Reports 2013 or SAP Crystal Reports for Enterprise designers. For universe connection information, use the Information Design Tool (.unx) or Universe design tool (.unv).
The version, support package, and patch level of the source system.	On Windows this can be determined by looking at the *Remove or Change* programs tool. On Unix, you can use the `modifyOrRemoveProducts.sh` utility in the BI platform installation directory.
The file store locations for every Input FRS and Output FRS in the deployment.	Go to the *Servers* tab of the CMC, right-click the Input or Output FRS and select *Properties*. Look for the *File Store Directory* property. **Note** If the value begins with % then this is a placeholder, and you will need to click on *Placeholders* and make a note of the directory listed under that placeholder.
If you plan to copy Promotion Management, the location of the Promotion Management database folder and Subversion folders.	The default folder for the Promotion Management database in Windows installations is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride` and on Unix it is **<INSTALLDIR>**`/sap_bobj/data/LCM/LCMOverride`. The default locations for the Subversion files in Windows installations are: • **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\CheckOut` • **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository` and on Unix they are: • **<INSTALLDIR>**`/check_out` (This directory is created only after you have used Subversion to check out files.) • `$HOME/LCM_Repository`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Location
If you plan on copying the monitoring database, the monitoring database folder.	This is set in the CMC. Go to the *Applications* management area of the CMC, Select *Monitoring Application* > *Properties* and look for the *Trending database backup directory*. The default folder in Windows installations is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB and on Unix it is **<INSTALLDIR>**/sap_bobj/Data/TrendingDB.
The semantic layer folder path.	The default folder path in Windows installations is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\ by default.

After you've recorded the information above:

1. Use your database vendor backup tools to create a backup copy of the following databases:
   - The CMS system database
   - The auditing database (optional)
2. Using file backup tools, back up the following sets of files:
   - The FRS input and output file stores.
   - The monitoring trending database (optional). This can be achieved by backing up files from the monitoring folder as recorded on the worksheet. By default, on Windows it is: **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. On Unix: **<INSTALLDIR>**/sap_bobj/Data/TrendingDB.
   - Promotion management database (optional). This can be achieved by backing up files from the database folder as recorded on the worksheet. By default, on Windows it is: **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride. On Unix: **<INSTALLDIR>**/sap_bobj/data/LCM/LCMOverride.
   - Promotion management Subversion database (optional). This can be achieved by backing up files from the Subversion folders as recorded on the worksheet. By default, on Windows they are:
     - **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\CheckOut
     - **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository.

     And on Unix they are:
     - **<INSTALLDIR>**/check_out (This directory is created only after you have used Subversion to check out files.)
     - $HOME/LCM_Repository
   - 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> For constraints and a detailed description of this workflow, please see the Hot backups [page 446] section.

3. The following files are user-customizable. If you have customized any of them, back up the files from the source system, and later restore them to the same folder on the target system:
   - `BO_trace.ini` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
   - `clientSDKOptions.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
   - `mdas.properties` installed to:
     - `[INSTALLDIR]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
   - WDeploy configuration files installed to `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf`:
     - `config.apache`
     - `config.jboss7`
     - `config.sapappsvr73`
     - `config.tomcat6`
     - `config.tomcat7`
     - `config.weblogic11`
     - `config.websphere7`
     - `config.websphere8`
     - `wdeploy.conf`
4. The following web-tier files are user-customizable. If you have made changes to any of these files, back up the files from the source system. Later, you will need to restore these files or reapply the changes to the target system.
   - `BO_trace.ini` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
   - `clientaccesspolicy.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
   - `clientSDKOptions.xml` installed to:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
- `crossdomain.xml` installed to:
  - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
  - `[INSTALLDIR]tomcat/webapps/ROOT`
- Any customized files in the `config/custom` folder (in the web tier). Back up these files to transfer the customization to the target system.

5. Back up any custom extensions that you've manually added to the source system; for example, publication extensions, custom libraries, and so on.

Keep the information recorded above with the copy of the databases and files. You may want to keep a second copy which you can update as required for future system copy procedures.

14.6.2 To import to a target system

This procedure assumes you have created backup copies of the source deployment databases and system files you want to use in your target system. All backup files must be from the same backup set. You will also need the details (cluster key and database credentials for example) noted in "To export from a source system".

If the target system will reside in a network location with access to the source system resources, you should ensure the target system does not attempt to access those resources until it has been reconfigured. This can be accomplished by placing a firewall between the target system and the source system resources, or leaving the source system stopped while you start the target system. After the first time you start the target system, the firewall can be removed or the source system can be started.

If the target system already has the BI platform installed, ensure it is at the same version, support package, and patch level as the source system at the time the copy was created. Also ensure it uses the same installation path as the source system.

1. On the target system, create the connections to the database or databases where you intend to put the CMS repository, auditing database, and reporting database.

   > **Note**
   >
   > While the connections can point to a different database, they must have the same connection name or DSN and use the same credentials as the source system.

2. Use your database tools to restore the CMS system database and the auditing database (if required) from the source-system backup to the target database.

   If the universes or reports on the target system need to use a different reporting database, modify the database connection to point to that database.

   If you require further instructions on this step, see the Restoring your system [page 451] topic.

3. If the BI platform is installed on the target host system, skip to Step 4. If the BI platform is not installed, install the BI platform on the target host system keeping the following steps in mind:
   a. Install the same program version, support package, and patch level as the source system.
   b. Use the same installation path as the source system.
   c. Select the same components that were installed on the source system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

d. When the installation program asks you to create the CMS database (and auditing database if applicable), choose the *Use an existing database server* option and enter the connection name and credentials set up in step 1.

> **Note**
>
> Do not choose to reinitialize the CMS database.

e. When prompted for the *Node Name*, use the same names, port numbers, platform administrator password and cluster key as the source system.

   For complete installation instructions, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. When the system has finished installing, go to step 6.

> **Note**
>
> If you are not copying your auditing data from the source system, you can create a new auditing database by configuring auditing during the installation procedure.

f. Stop all nodes in the CCM.

4. If the BI platform is already installed on the target system, stop all nodes in the CCM. On the target system CMS host computer, start the CCM.
5. If the BI platform is already installed, add a new node, using the *Recreate Node* option.
   a. Use the *Node Name* and *SIA Port Number* from the source system.
   b. Choose to *Start a new temporary CMS*.
   c. Select a new *CMS Port Number* (can be any free port) and *CMS Database Type* (matching the restored database type).
   d. Enter details for the connection the CMS database was restored to in Step 1.
   e. Enter the cluster key from the source-system.
   f. Enter the Administrator password from the source system.
6. Restore the Input and Output FRS file stores to the target system file store. Use the same folder as was used on the source system.
7. Restore the monitoring database folder (if you want to copy monitoring information) to the same folder as was used on the source system.
8. Restore the Promotion Management database folder (if you want to copy Promotion Management information) to the same folder as was used on the source system.
9. Restore the Subversion files (if you want to copy Promotion Management information) to the same folder as was used on the source system.
10. Restore the semantic layer/connection configuration server files to the same folder as was used on the source system.
11. Restart the target system host computers.
12. If you installed the BI platform on the target system in step 3, apply any support packages or patches required to match the source system.
13. If the target system will run on multiple host computers, repeat steps 1–11 for each host computer.

    Use the Expand install option when installing additional BI platform nodes, and keep in mind that the same node names as the source system should be used for the additional nodes in the target system.
14. If the target system CMS database will use a different database type from the source system, use the CCM to perform Copying data from one CMS system database to another [page 402], specifying as destination the database you want to use for the copy.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15. Restore any user-customizable files that you backed up in step 3 of the procedure “To export from a source system”.
16. Restore any web-tier files that you backed up in step 4 of the procedure “To export from a source system”.

    “Web tier” refers to the WDeploy staging area where you can perform your customizations, and to the web-tier content that is deployed to the application server.

    When applying changes to the target system, do not apply changes to the application server directory; apply the changes to the WDeploy staging area, and then redeploy the web tier to the application server using WDeploy.

    The WDeploy staging area is this location on Windows: **<INSTALLDIR>**`/SAP BusinessObjects Enterprise XI 4.0/warfiles`.
17. Restore any extensions that you backed up in step 5 of the procedure “To export from a source system”.

After the system copy of the BI platform is performed:

1. The installation of the first node on the target creates a temporary CMS, which will be stopped at the end of the installation. Using the CMC, go to the Servers page and delete this CMS.

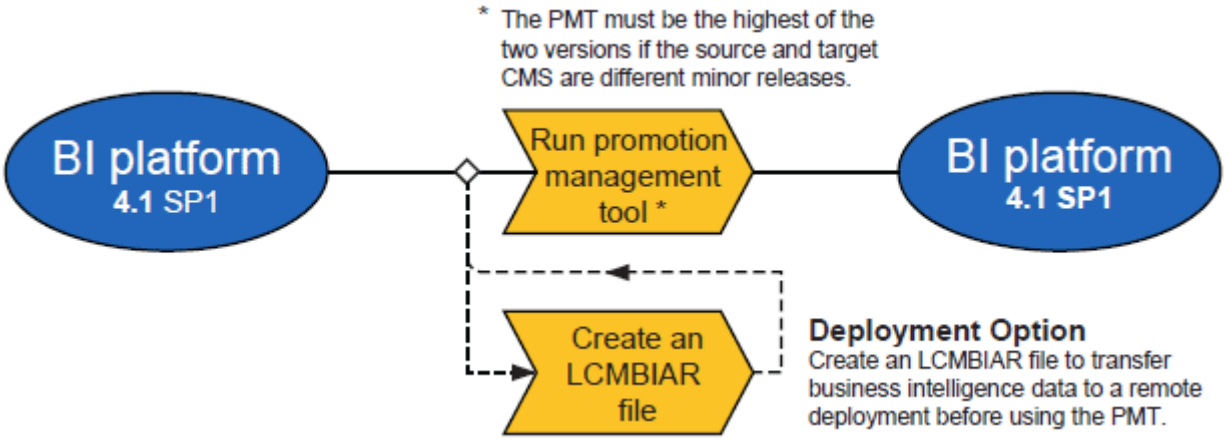
   > **Remember**
   >
   > If you do not remove the source system (or if you use it concurrently with the target system), renaming the cluster on the target system is recommended.
2. Run the Repository Diagnostic Tool on the target CMS database.
3. If applicable, configure Windows AD single sign-on (SSO) on the target system. See SSO to the BI platform with AD authentication [page 256].
4. If applicable, configure SLD on the target system. For details, see SAP Note 1508421: “SAP SLD Data Supplier for Apache Tomcat”.
5. Perform a sanity check on the target system to ensure its integrity.
6. Perform a full search re-index.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15 Promotion Management

15.1 Welcome to promotion management

15.1.1 Overview



The promotion management tool allows you to move business intelligence (BI) resources from one repository to another, manages dependencies of the resources and also rolls back the promoted resources at the destination system, if required. It also supports the management of different versions of the same BI resource.

The promotion management tool is integrated with the Central Management Console. You can promote a business intelligence resource from one system to another only if the same version of the BI platform is installed on both the source and destination systems.

15.1.2 Features

The promotion management tool allows you to perform the following actions on infoobjects in the destination desployment.

- Create a new job
- Copy an existing job
- Edit a job
- Schedule a job promotion
- View the history of a job
- Export as LCMBIAR
- Import both BIAR /LCMBIAR

The promotion workflow also includes the following tasks:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- *Managing Dependencies* This feature allows you to select, filter, and manage the dependents of the infoobjects in the job that you want to promote.
- *Scheduling* This feature allows you to specify a time for job promotion, rather than promote a job as soon as it is created. You can specify the job promotion to run once or on a recurring schedule.
- *Security* This feature allows you to promote infoobjects along with the associated security rights and if required promotes infoobjects associated with application rights.
- *Test Promotion* This feature allows you to check or test the promotion to ensure that all the preventive measures are taken before the actual promotion of the infoobjects.
- *Rollback* This feature allows you to restore the destination system to its previous state, after a job is promoted. You can roll back an entire job or a part of the job.
- *Auditing* The events generated by the promotion management tool are stored in the audit database. This feature enables you to monitor the events that are logged in the audit database.
- *Promotion Management Override Settings* This feature allows you to scan and promote the overrides through a job promotion.

15.1.3 Application access rights

This section describes the application access rights for the promotion management tool.

- You can set access rights to the promotion management tool within the CMC.
- You can set granular application rights to various functions within the promotion management tool.

To set specific rights in the promotion management tool, complete the following steps:

1. Log on to the CMC and select *Applications*.
2. Double-click *promotion management*.
3. Click *User Security*, and select a user. You can view or assign security rights for the user.
4. The following promotion management specific rights are available:
    - Allow access to edit overrides
    - Allow access to Include Security
    - Allow access to administration
    - Allow access to Manage Dependencies
    - Create Job
    - Delete Job
    - Edit Job
    - Edit LCMBIAR
    - Export as LCMBIAR
    - Import LCMBIAR
    - Promote Job
    - Rollback Job
    - View and Select BOMM (BusinessObjects Metadata) Objects
    - View and Select Business Views
    - View and Select Calenders
    - View and Select Connections
    - View and Select Profiles

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- View and Select QaaWS
- View and Select Report Objects
- View and select Security settings
- View and select Universes

5. If you wish to assign rights to a selected user, select the appropriate right and click *Assign Security*.

The promotion management tool access rights are set within the CMC.

15.1.4 Support for WinAD in promotion management

In order for the promotion management tool to function properly, you must add the following to all `javaargs` arguments for all Adaptive Job Servers:

```
Djava.security.auth.login.config=<path>
\bsclogin.conf,Djava.security.krb5.conf=<path>\krb5.ini
```

> **Remember**
>
> Specify the correct path to `bsclogin.conf` and `krb5.ini` on your deployment.

15.1.5 Override information in BI platform 4.1 SP3 and newer

From BI platform 4.1 SP3, the Derby database is replaced with information stored in the repository. During promotion from 4.0 SPx, or 4.1 SPx, a silent, automatic promotion takes place.

If the automatic promotion fails (for example, if the APS displays errors after promotion), you can manually set the forced migration flag:

1. Stop the Adaptive Processing Server (APS) running Promotion Management.
2. Add the `-Dcom.businessobjects.lcm.migrateoverrides=true` parameter to the APS.
3. Start the APS and let the forced migration to take place.

> **Remember**
>
> When the migration is complete, remove the parameter from the APS.

15.1.6 To override connections between the Application Server and the Message Server

You can override the Application Server to connect to the Message Server or the Message Server to connect to the Application Server by setting parameters in the*Edit Common Connection Properties* dialog.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Depending on your system configuration, you may also need to update the following fields common to both the Application Server and Message Server: *CLIENT*, *SYSID*, *USERNAME*, and *PASSWORD*.

1. (Optional) To override the Application Server to connect to the Message Server, set the following parameters:

GROUP	**<GROUP>**
SERVERTYPE	**GROUP**
MSHOST	**<MESSAGESERVER>**

> **Note**
>
> You can also clear the *ASHOST* and *SYSNR* fields.

2. (Optional) To override the Message Server to connect to the Application Server, set the following parameters:

SERVERTYPE	**SERVER**
ASHOST	**<APPLICATIONSERVER>**
SYSNR	**<SYSTEMNUMBER>**

> **Note**
>
> You can also clear the *GROUP* and *MSHOST* fields.

15.2 Getting started with the promotion management tool

15.2.1 Accessing the promotion management tool

To access the promotion management tool, select *Promotion Management* from the CMC home page.

Any user with view permissions to the *Promotion Jobs* folder can launch the promotion management tool. However, to create, schedule, or promote a job, the user must be granted additional rights by the administrator.

15.2.2 User interface components

This chapter discusses the GUI components in the promotion management tool.

- promotion management workspace toolbar
- Workspace panel
- Tree panel
- Details panel

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Shopping Cart and Job Viewer page

Promotion management workspace toolbar

The following table lists the options included in the promotion management workspace toolbar and discusses the tasks you can perform using these options:

Table 76:

Option	Description
	allows you to create a new folder. The new folder is created as a subfolder in the *Promotion Jobs* folder.
	allows you to copy and remove the selected job or folder from its current location.
	allows you to copy the job or folder from its current location.
	allows you to paste the copied job or folder in a new location.
	allows you to delete an existing job or folder.
	allows you to refresh the home page, to obtain the updated list of jobs or folders.
Properties	allows you to modify the properties of the selected job. You can modify the title, description, and keywords of the selected job.
History	allows you to view the history of the selected job.
New Job	allows you to create a new job.
Import	allows you to import a BIAR, LCMBIAR, or Override files.
Edit	allows you to edit the selected job.
Promote	allows you to promote the selected job.
Rollback	allows you to undo the promoted job on the destination system. **Note** If the job promotes objects to the destination, rollback will delete these objects. If the job updates objects on the destination, rollback will restore the previous version of the objects.
	allows you to navigate between pages of a job list. You can use this option to navigate a single page, or navigate to a specific page by entering the relevant page number.
Search	allows you to search for specific jobs. You can search for a job by its name, keywords, description, or all three parameters.
Promotion Jobs	allows you to view the jobs and folders.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Promotion Status	Displays the promoted jobs according to their status, such as Success, Failure, or Partial Success.

Workspace panel

The Workspace panel in the promotion management home page displays the list of jobs. You can use this panel to view the name, status, creation time, and last run time of the job, the source and destination systems, and the job creator.

Tree panel

The Tree panel in the promotion management home page displays the tree structure, which includes the *Promotion Job* folder and the *Promotion Status* folder. The jobs are displayed in a hierarchical structure under the *Promotion Job* folder. The *Promotion Status* folder displays the promoted jobs according to their status.

Job Viewer page

The “Job Viewer” page is displayed when a user creates a new job or edits an existing job. It contains a dynamically-generated list of infoobjects to be promoted and a details panel. The list categorizes the infoobjects into user groups, universes, and connections. The details panel shows the contents of the node selected from the list.

15.2.3 Using the Settings option

The Settings option allows you to configure settings before promoting infoobjects from one BI platform deployment to another BI platform deployment and SAP deployment. This section describes how to use the settings options.

Click the *Settings* drop-down in the *Promotion Jobs* screen. This drop-down displays the following options:

- *Manage Systems* This option allows you to add all the systems required for promotion management activities.
- *Rollback Settings* This option allows you to select a system for which rollback is enabled.
- *Job Settings* This option allows you to view completed instances onthe Dependencies page and allows managing job instance cleanup activities. It also allows filtering by job creation date.
- *CTS settings* This option allows you to add the web service and SAP BW system information for the Enhanced Change and Transport System integration.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.2.3.1 To use the Manage Systems option

This section describes how to use the Manage Systems option. You can add or remove host systems using this option.

To add a host system, complete the following steps:

1. On the promotion management workspace toolbar, click *Settings* and then click *Manage Systems*.
   The *Manage Systems* window is displayed. This window displays a list of host names, port numbers, display names, and descriptions.
2. Click *Add*.
   The *Add System* dialog box is displayed.
3. Add the host name, port number, display name, and the description in the appropriate fields.

   > **Note**
   >
   > Select the *Mark as 'Origin'* option to identify the system as a source system (the system where the connection information originated from). This option is useful for working with overrides.

4. Click *OK* to add the system.
   The host system is added to the list.

> **Note**
>
> To remove or edit a host system, select a host system and click *Remove* or *Edit*.

Related Information

To use the Rollback Settings option [page 479]
To use the Job Settings option [page 480]

15.2.3.2 To use the Rollback Settings option

By default, the rollback process is enabled at the system level. The *Rollback Settings* option allows you to disable the rollback process at the system level.

To disable the rollback process at the system level, complete the following steps:

1. In the *Rollback* window, from the list of host systems, select the host system to disable the rollback process.
2. Click *Save and Close* to save the modifications.

Related Information

To use the Job Settings option [page 480]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.2.3.3 To use the Job Settings option

The Job Settings option allows you to specify whether you want to show completed instances on the “Manage Dependencies” page and the number of job instances that can exist in the system. You can specify one of the following options:

- *Show completed instances in Manage Dependencies page* This option allows viewing completed instances on the “Manage Dependencies” page that can be added to the job.
- *Delete Instances when more than N instances of a Job* This option allows specifying the maximum number of job instances per job in the system.
- *Delete Instances after N days for the Job* This option allows specifying the job instances created before a specified number of days to be deleted.
- From the *Show Jobs Created* list, you can select the time interval to view the jobs created during the specified period.

To set the *Job Settings* option, complete the following steps:

1. Select the option, and enter the preferred value.
2. Click *Save* to save the updated changes.

You can click *Default Settings* to set the default values, and you can click *Close* to close the window.

> **Note**
>
> The old job instances are deleted only when the job is executed the next time.

Related Information

To use the Version Management System settings option [page 530]

15.2.3.4 Using the Override Settings option

The Override Settings option allows promoting overrides using a job promotion or an LCMBIAR file. This option allows scanning, promoting, and editing the database connection information for Crystal Reports and Universe connections. You can also use it to edit the QAAWS URLs.

> **Note**
>
> To use the Override Settings option, you must install Adobe Flash Viewer.

The term *system* is used in the following procedures. There are three types of systems:

- *Origin* The originating system for any connection information.
- *Central Promotion Management* The system which runs the Promotion Management tool.
- *Destination* The end system to which the BI resources are promoted.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.2.3.4.1 To promote overrides

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 479].

To promote the overrides, complete the following steps:

1. On the promotion management workspace toolbar, click the *Override Settings* option.
   The *Override Settings* window is displayed.
2. If you are logged on to the Central promotion management system, log out from the system.
3. Click *Login* to connect to the Origin system.
   The *Login to system* window is displayed.
4. Select the source system marked as *Origin* to scan the objects, and login to the system using valid credentials.
5. From the *Start* dropdown list next to *Scan*, select the *Start* option.
   The scanning process starts. The *list of unique connections* is displayed.

   > **Note**
   >
   > To schedule a recurring scan, select *Recurrence Settings* option from the drop-down list.

6. In the list of overrides, change the status to Active for the objects you want to promote, and click *Save*.
7. Click *Promote Overrides*.
   The *Promote Overrides* screen is displayed where the list of destination systems is displayed.
8. Click *Login* to log into the destination system using valid credentials.

   You can specify multiple destination systems.
9. Click *Promote*.
   The promotion of overrides is complete.

   > **Note**
   >
   > If the overrides fail at the destination system during the promotion of infoobjects, the system sets the job status to `Partial Success` and also sets the `Overrides Failed` warning status on the object.

10. Log off from the Origin system.
11. From the *Override Settings* screen, click *Login* .
    The Login to System window is displayed.
12. Login to one of the destination systems using valid credentials.
    A list of all the promoted objects is displayed in a *list of unique connection*. The status of these objects is Inactive.
13. Click the *Select* check box for the objects you want to edit, and click *Edit*.
14. Update the required values, and click *Done*.
    The state of the edited objects becomes Active.
15. Click *Save*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.2.3.4.2 To promote overrides using BIAR Files

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 479].

To promote the overrides through BIAR files, complete the following steps:

1. On the promotion management workspace toolbar, click the *Override Settings* option.
   The *Override Settings* window is displayed.
2. If you are logged on to the Central Promotion Management system, log out from the system.
3. Click *Login* to connect to the Origin system.
   The *Login to system* window is displayed.
4. In the *Override Settings* screen, select the source system marked as *Origin* to scan the objects and login to the system using valid credentials.
5. From the *Start* drop-down list next to *Scan*, select the *Start* option.
   The scanning process starts.The List of Overrides is displayed.

   > **Note**
   >
   > To schedule a recurring scan, select *Recurrence Settings* option from the drop-down list.

6. In the list of overrides, change the status of the required objects to Active, and click *Save*.
7. Click *Promote Overrides*.
   The *Promote Overrides* screen is displayed where the list of destination systems is displayed.
8. To encrypt the BIAR file using a password, click *Password Encryption* checkbox.
   The *Password* and *Confirm Password* fields are enabled.
9. Enter a password in the *Password* field. Re-enter the same password in the *Confirm Password* field.
10. Click *Export*, and save the overrides BIAR file to a file system.
11. Log into the destination system through the CMC, and in the promotion management tool click *Import* > *Override File*.
    The *Import LCMBIAR file* window is displayed.
12. Click *Browse* to browse the BIAR file.
13. Enter the password of the BIAR file in the *Password* field.

    > **Note**
    >
    > The *Password* field is displayed only if the BIAR file you selected is encrypted using a password

14. Click *OK*. The promotion of overrides is complete.
15. Log off from the origin system.
16. From the *Override Settings* screen, click *Login*.
    The *Login to system* window is displayed.
17. Login to the destination system using valid credentials.
    A list of imported objects is displayed in List of Overrides.The status of these objects is Inactive.
18. Click the *Select* check box for the objects you want to edit, and click *Edit*. The edited objects are indicated by an icon.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> You can delete the override objects by clicking on the icon.

19. Update the required values, and click *Done*.
    The state of the edited objects becomes Active.
20. Click *Save*.

15.2.3.4.3 To promote overrides using CTS+

Add a host system before promoting the overrides. For information about adding host systems, see To use the Manage Systems option [page 479].

To promote the overrides through CTS+, complete the following steps:

> **Note**
>
> Launch the promotion management tool using SAP authentication for this option to be available.

1. On the promotion management workspace toolbar, click the *Override Settings* option.
   The *Override Settings* window is displayed.
2. If you are logged on to the Central Promotion Management system, log out from the system.
3. Click *Login* to connect to the Origin system.
   The *Login to system* window is displayed.
4. Select the source system marked as *Origin* to scan the objects, and login to the system using valid credentials.
5. From the *Start* drop-down list next to *Scan*, select the *Start* option.
   The scanning process starts. The *List of Overrides* is displayed.

   > **Note**
   >
   > To schedule a recurring scan, select *Recurrence Settings* option from the drop-down list.

6. In the list of overrides, change the status to Active for the objects you want to promote, and click *Save*.
7. Click *Promote Overrides*.
   The *Promote Overrides* screen is displayed where the list of destination systems is displayed.
8. From the *Promotion Options* drop-down list, select *Promote with CTS+*.
9. Click *Promote*.
10. Release the overrides to the destination system by completing the following steps:
    a. Login to the domain controller of CTS+ and open the *Transport Organizer* Web UI. For more information on using the Transport Organizer Web UI, see Transport Organizer Web UI.
    b. If the status of the request is *Modifiable*, click *Release* to release the transport request of the overrides. For more information on Releasing Transport Requests with Non-ABAP Objects, see Releasing Transport Requests with Non-ABAP Objects.
    c. Close the *Transport Organizer* Web UI.
11. Import the overrides to the destination system by completing the following steps:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

a. Login to the Domain Controller of CTS+.
b. Call the STMS transaction to enter the transport management system.
c. Click on the *Import Overview* icon.

   The *Import Overview* screen is displayed and you can view the import queue items from all the systems.
d. Click the System ID of the destination Promotion Management system.
   You can see the list of transport requests that can be imported to the system.
e. Click *Refresh*.
f. Import the relevant transport requests. For more information, see the Importing Requests documentation.

12. The promotion of overrides is complete.
13. Login to one of the destination systems using valid credentials.
    A list of all the promoted objects is displayed in "list of overrides". The status of these objects is Inactive.
14. Click the *Select* check box for the objects you want to edit, and click *Edit*.
15. Update the required values, and click *Done* .
    The state of the edited objects becomes Active.
16. Click *Save*.

15.2.3.5 Using the CTS Settings option

You can use this option to add web services and manage BW systems in your landscape. Refer to the To configure CTS+ settings in the promotion management tool [page 519] section for more information on using the CTS Settings Option and setting up CTS for usage with the promotion management tool.

15.3 Using the promotion management tool

When you launch the promotion management tool, by default, you are taken to the *Promotion Jobs* page.

The *Promotion Jobs* home page screen includes various tabs that enable you to perform the following tasks:

- Click *New Job* to create a new job. You can also right-click the home page screen and select *New Job* from the list.
- Click *Import* > *Import file* to import a BIAR file or LCMBIAR directly from the file system, instead of performing the entire procedure of creating a new job.
- Click *Import* > *Override File* to import overrides.
- Select an existing job from the list and click *Edit* to edit the selected existing job.
- Select an existing job from the list and click *Promote* to promote the job from the source system to the destination system, or export the job to an LCMBIAR file.
- Select an existing, previously-run job from the list and click *Rollback* to revert the promoted objects from the destination system.
- Select an existing, previously-run job from the list and click *History* to view the previous promotion instances of the selected job.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Select an existing job from the list and click *Properties* to view the properties of the selected job, such as title, ID, file name, and description.

The *Promotion Jobs* application area displays the list of jobs and folders that exist in the system, along with the following information for each job or folder:

- *Name:* Displays the name of the job or folder that was created.
- *Status:* Displays the status of the job, such as Created, Success, Partial Success, Running, or Failure.
- *Created:* Displays the date and time when the job or folder was created.
- *Last Run:* Displays the date and time when the job was last promoted.
- *Source System:* Displays the name of the system from which the job is promoted.
- *Destination System:* Displays the name of the system to which the job is promoted.
- *Created By:* Displays the name of the user who created the particular job or folder.

> **Note**
>
> The promotion management tool uses the BI platform SDK for all of its activities.

15.3.1 Creating and deleting folders

This section describes how to create and delete a folder in the promotion jobs home page.

15.3.1.1 To create a folder

This section describes how to create a folder.

To create a folder, complete the following steps:

1. In the promotion management toolbar, click .
2. In the *Create Folder* dialog box, enter the folder name.
3. Click *OK*.

A new folder is created.

Related Information

To create a job [page 486]
To delete a folder [page 486]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.3.1.2 To delete a folder

This section describes how to delete a folder.

To delete a folder, complete the following steps:

1. Select a folder in the *Promotion Jobs* home page.
2. Click .
   The confirmation dialog box is displayed.
3. Click *OK*.

The selected folder is deleted.

Related Information

To create a job [page 486]

15.3.2 To create a job

This section describes how to create a new job by using the promotion management tool.

The following table discusses the GUI elements and fields that you can use to create a new job:

Table 77:

Field	Description
Name	Name of the job that you want to create.
Description	Description of the job you want to create.
Keywords	The keywords for the contents of the job you want to create.
Save Job in	The default selected folder is displayed.
Source System	The name of the BI platform system from which you want to promote a job.
Destination System	The name of the BI platform system to which you want to promote a job.
User name	The login ID that you must use to log into the source or destination system.
Password	The password that you must use to log into the source or destination system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Field	Description
Authentication	The authentication type that is used to log into the source or destination system. The promotion management tool supports the following authentication types: • Enterprise • Windows AD • LDAP • SAP

> **Note**
>
> Prior to job creation, ensure that the overrides, if any, have been edited and updated in the destination system so that the BI platform content is automatically updated. For more information see, Using the Override Settings Option.

To create a new job using the promotion management tool, complete the following steps:

1. Launch the promotion management tool.
2. In the *Promotion Jobs* home page, click *New Job*.
3. Enter the name, description, and keywords for the job in the appropriate fields.

   > **Note**
   >
   > Providing information in the Description, Keywords, and Destination System fields is optional.

4. In the *Save Job in* field, browse and select the folder in which you want to save the job.

   > **Note**
   >
   > By default, the *Save Job in* field will be populated by the name of the folder highlighted in the folders pane prior to clicking *New Job*.

5. Select source system and destination system from the respective drop-down lists.
   If the name of the system is not included in the drop-down list, click the *Login to a new CMS* option. A new window is launched. Enter the name of the system along with the user name and password.
6. Click *Create*.
   The "Add Objects" window is displayed.
7. Select the objects from the source system to be added to te job, and then click *Add & Close*.
8. Click *Save*.

The newly created job is stored in the CMS repository of the source system.

> **Note**
>
> If you create a job with a folder as the primary object and the job is a recurring one, the job will include any content added to the folder at the next run-time.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Using the Override Settings option [page 480]

15.3.2.1 To log onto a new CMS

This section describes how to log into a new CMS.

To log into a new CMS, complete the following steps:

1. Launch the promotion management application.
2. Create a new job.
   For more information on creating a new job, see To create a job [page 486].
3. From the *Source System* drop-down list, select *Login to a New CMS*.
   The *Login to System* dialog box is displayed.
4. Select the system from the drop-down list or type in a new system name.
5. Enter the user credentials, select the appropriate authentication type, and click *Login*.
6. From the *Destination System* drop-down list, select *Login to a New CMS*.
7. Select the system from the drop-down list or type in a new system name.
8. Enter the user credentials, select the appropriate authentication type, and click *Login*.

Related Information

To edit a job [page 489]
To add an infoobject to a job [page 490]
To promote a job when repositories are connected [page 492]
To schedule a job promotion [page 497]

15.3.3 To create a new job by copying an existing job

This section describes how to create a new job by copying an existing job.

To create a new job by copying an existing job, complete the following steps:

1. Launch into the promotion management tool.
2. In the *Promotion Jobs* home page, click *New Job*.
3. Click the *Copy an Existing Job* option.
   The *Copy an Existing Job* window is displayed displaying the list of jobs in the *Promotion Jobs* folder.
4. Select the required job from the list, and click *Create*.
   The name, keywords, and description of the job, as well as the *Save Job In* and *Destination* fields are displayed. You can modify these fields as necessary.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. In the *Save Job in* field, browse and select the folder in which you want to save the job, and click *Create*.

A new job is created, and the *Add Objects* window is displayed.

Related Information

To add an infoobject to a job [page 490]
To edit a job [page 489]
To promote a job when repositories are connected [page 492]

15.3.4 To search for a job

The search feature in the promotion management tool allows you to locate a job that is available in the repository.

To search for a job, complete the following steps:

1. In the *Search* field of the home page, enter the text that you want to locate.
2. Click the list that is displayed beside the *Search* field to specify the search parameters. You can specify the following search parameters:
   - *Search Title* This option allows you to search for a job by its name.
   - *Search Keyword* This option allows you to search for a job by its keywords.
   - *Search Description* This option allows you to search for a job by its description.
   - *Search All Fields* This option allows you to search for a job by its title, keywords, and description.
3. Click the Search icon.

Related Information

To add an infoobject to a job [page 490]
To edit a job [page 489]

15.3.5 To edit a job

This section describes how to edit a job.

> **Note**
>
> Editing a job does not amount to creating a new job.

To edit a job, complete the following steps:

1. Launch into the promotion management tool.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. In the *Promotion Jobs* home page, select the job that you want to edit.
3. Click *Edit*.
   The details of the selected job are displayed. You can add or remove infoobjects, manage dependencies or promote the job, as necessary.

While editing a job, you cannot change the name of the source system.

Related Information

To add an infoobject to a job [page 490]
To promote a job when repositories are connected [page 492]
To schedule a job promotion [page 497]

15.3.6 To add an infoobject to a job

Each job must include a set of infoobjects. Hence, you must add infoobjects to a job before you promote it to the destination system.

> **Note**
>
> When you promote a Crystal report based on Business View infoobjects (Data Connection, Data Foundation, Business Elements, and Business View) you must include the security information (DataAccess right on Data Connection and the ViewDataField right on Data Foundation and Business Elements) to see data in a report on the destination system.

To add an infoobject to a job, complete the following steps:

1. Launch the promotion management tool.
2. Create a new job or edit an existing job.
   For information on creating a new job, see To create a job [page 486] and To edit a job [page 489].
3. Click *Add Objects* if editing a job.

   > **Note**
   >
   > The *Add Objects* dialog box is displayed when creating a new job..

4. Navigate to the folder from which you want to select the infoobject.
   The list of infoobjects in the selected folder is displayed.
5. Select the infoobject that you want to add to the job, and click *Add*

   If you want to add an infoobject and exit the "Add Objects from the System: `<NAME>`" dialog box, click *Add and Close*. The infoobject is appended to the job and the dialog box closes.

After you add an infoobject to a job, you can right-click the *Job Viewer* page and select promotion processes to proceed with the promotion task. You can manage the dependents of the infoobject you selected using the *Manage Dependencies* option in the *Job Viewer* page.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> - The Shopping Cart, which is displayed in the left panel of the *Job Viewer* page, displays the job, along with its dependents, in a flat tree structure.
> - Click *Save* option after adding infoobjects, to save the changes. Otherwise, the user is prompted with an option to save the job when the user closes the tab.

Best Practice: SAP BusinessObjects recommends that you select a small number of infoobjects, which should not exceed 100 at a time, for promotion to obtain optimum performance of the promotion management tool.

Related Information

To manage the dependencies of a job [page 491]
To promote a job when repositories are connected [page 492]
To schedule a job promotion [page 497]

15.3.7 To manage the dependencies of a job

This section describes how to manage the dependents of an infoobject.

To manage the dependents of an infoobject, complete the following steps:

1. Launch the promotion management tool.
2. Create a new job or edit an existing job.
   For information on creating a new job, see To create a job [page 486] and To edit a job [page 489].
3. Add the required infoobjects to the job and close the *Add Objects* dialog to return to the *Job Viewer* window.
4. Click *Manage Dependencies*.
   The *Manage Dependencies* window is displayed. This window displays the list of infoobjects and their dependents. To view only the object dependents that have not been selected, click *Show unselected Dependents* check box.
5. From the *Select Dependents* drop-down list, select the options to add the grouped dependents to the job. The dependents are not selected by default; you must explicitly select the dependents you want to promote.

   For example, if you select *All Universes* from the *Select Dependents* drop-down list, then all universes included in the list of dependents are selected. You can also select the dependents individually.

   You can click the *Type* to view the supported filtering options for the infoobjects. A drop-down list is displayed. This list displays the supported filtering options. Select the filtering option, and click *OK*. The filtered infoobjects are displayed.

   When you select the dependents from the *Dependents* column, and click *Apply Changes* the dependents are automatically moved to the *Objects in Job* column.

   You can also type the name of the dependent in the *Search Dependents* field to search for a dependent.

   For more information on searching for dependents, see To search for dependents [page 492]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Click *Apply Changes* to update the list of dependents and click *Apply Changes and Close* to save the changes.

Dependent objects are computed automatically by the tool. These dependents are computed based on either the infoobject relationships or infoobject properties. Dependents that do not qualify under either of these are not computed in this version of the tool.

> **Note**
>
> If you select a folder for promotion, then the contents in the selected folder are considered as primary resources.

Related Information

To promote a job when repositories are connected [page 492]

15.3.8 To search for dependents

The advanced search feature in the promotion management tool allows you to locate the dependents of infoobjects that are available in the repository.

To search for the dependents of an infoobject, complete the following steps:

1. Launch promotion management.
2. Create a new job, or edit an existing job.
   If you have created a new job, add infoobjects to the job. If you are editing an existing job, you can add objects, as necessary.
3. Click *Managing Dependencies*.
4. In the *Search Dependents* field, enter the name of the dependent you want to locate.
5. Click the Search icon.

Related Information

To manage the dependencies of a job [page 491]

15.3.9 To promote a job when repositories are connected

This section describes how to promote a job from the source system to the destination system if both systems are live.

The following table lists the infoobject types that can be promoted using the promotion management tool:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 78:

Category	Object types you can promote
Reports	Crystal reports, Web Intelligence, Dashboards, QaaWS, Explorer
Third-Party Objects	Rich text, Text document, Microsoft Excel, Microsoft Power Point, Microsoft word, Flash, Adobe acrobat
Users	Users and user groups
Server	Server groups
Business Intelligence Platform	Folder, Program, Events, Profiles, Object package, HyperLink, Categories, Inbox document, Personal and Favorites folder
Universe, Workspace	Universes UNV, Connections
EPM Dashboard	Universes, Connections, Reports, Dashboard, and Analytics
BusinessView	DataFoundation
Federation • Replication List • Replication Jobs	Replication List promotes the following objects: Flash, .txt, Discussions, Dashboards, .pdf, Hyperlink, .xls, ObjectPackage, Crystal Reports, Web Intelligence Documents, Universes, Program, Connections, DataFoundation, Business Views, .rtf, Profile, Event, Users, and userGroups. Replication Connections promotes Replication Jobs, Remote Connection, Publications, Discussion, Pioneer Connection
BI Services	Web Intelligence Documents, Universes and Connections
New Infoobjects	Crystal reports (rpt/rptr),Pioneer, Dashboard Design, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Data Fooundation (DFX), WebI, Explorer, Data Federator, Data Steward, BI Workspace, etc.

To promote a job, complete the following steps:

1. Launch promotion management.
2. In the *Promotion Jobs* home page, select the job you want to promote.
   You can also right-click the home page screen, and click *Promote*.
3. From the *Destination* system list, select a different destination system as necessary.

   > **Note**
   >
   > Ensure that you have logged into both source and destination systems before you proceed with promotion process.

4. In the *Change Management ID* field, enter the appropriate value, and click *Save*.

   > **Note**
   >
   > The Change Management ID is used for obtaining information related to logging, auditing, job history. The promotion management tool allows you to map each instance of job creation to a Change Management ID. The Change Management ID is an attribute that is set by the user in the job definition while creating a new job. The tool automatically generates an ID for each job.

5. Select *Security Settings*, as necessary. The following options are displayed:
   - *Do not promote security* This is the default option.
   - *Promote security* Use this option to promote jobs along with the associated security rights.
   - *Promote object security* Use this option to promote the security of objects and folders

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- *Promote user security* allows you to promote the rights of the users who are a part of the job
- *Include Application Rights* You can select this option only when you also select *Promote User Security*. If the objects in the job inherit any application rights, the job is promoted along with those rights.

You can also click *View Rights* to view the security dependencies of infoobjects in the job.

6. Click *Test Promote* to ensure that there are no conflicts between CUIDs of infoobjects in the source and destination systems. The promotion details are displayed under the tabs *Success*, *Failure* and *Warning*. The first column displays the objects to be promoted, and the second column displays promotion status of each infoobject. The promotion management tool classifies the selected objects into users, groups, universes.

   > **Note**
   >
   > This option does not commit any infoobjects for promotion.

   The result of a test promote can be any one of the following:

   - `Overwritten` The infoobject in the destination system is overwritten by the infoobject in the source system.
   - `Copied` The infoobject in the source system is copied to the destination system.
   - `Dropped` The infoobject is not promoted from the source system to the destination system.
   - `Warning` The infoobject in the destination system is the newer version and you can remove the infoobject from the Job. However, if you want to promote, the infoobject gets promoted.
   - `Mapped` The infoobject is mapped to an infoobject on the destination system.
7. Click *Schedule* if you want promotion to run at a specific time or on a recurring schedule.
8. Click *Promote*.
   The selected job is promoted.

If you do not want to promote the job, you can use the *Save* option to save the modifications such as Security, Change Management ID, and Schedule settings.

15.3.10 Promoting a job using an LCMBIAR File

Promoting refers to the activity of transferring a BI resource from one repository to another. If the source system and destination system are on the same network, the promotion management tool uses WAN or LAN to promote the infoobject. However, the promotion management tool also facilitates the promotion of infoobjects even if the source and destination systems are not on the same network.

In scenarios where the source and destination systems are not on the same network, the promotion management tool supports the promotion of jobs to the destination system by enabling you to export the job in the source system to an LCMBIAR file and import the job from the BIAR file to the destination system.

This section describes how to export a job to an LCMBIAR file and then import the job from the BIAR file to the destination system.

> **Note**
>
> You cannot use an LCMBIAR file that was created using the Import Wizard.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Exporting a job to an LCMBIAR File [page 495]
Importing a job from an LCMBIAR File [page 495]

15.3.10.1 Exporting a job to an LCMBIAR File

This section describes how to export a job to an LCMBIAR file.

To export a job to an LCMBIAR file, complete the following steps:

1. Launch the promotion management tool, and create a new job.
   For more information on creating a new job, see To create a job [page 486]
2. From the *Destination* drop-down list, select *Output to LCMBIAR file* option and click *Create*.
3. Click *Add Objects* to add infoobjects to the job.

   You can use the *Manage Dependencies* option to manage the dependencies of the selected job.
4. To encrypt the LCMBIAR file using password, click *Password Encryption* checkbox.
5. Enter a password in the *Password* field.
6. Re-enter the password in the *Verify Password* field.
7. Click *Promote*.
   The *Promote* window is displayed.
8. Modify the security options as needed and click *Export*.
   The LCMBIAR file is created. You can save the LCMBIAR file to the file system.
9. (Optional) Click *LCMBiar File Destination* and select *FTP* to export the LCMBIAR file to an FTP server. Enter the hostname, port, username, password, directory, and filename and click *Export*.
10. From the *Destination* drop-down list, select *Output to LCMBIAR file*, and click *LCMBIAR File Destination*.

You can schedule the export of a job to an LCMBIAR file. For more information on this, refer to the To schedule a job promotion [page 497] section.

Related Information

To add an infoobject to a job [page 490]
To manage the dependencies of a job [page 491]

15.3.10.2 Importing a job from an LCMBIAR File

You can import a job from an LCMBIAR file. The LCMBIAR file is copied from the storage device to the destination system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> You can also import a job from an upgrade management tool BIAR file.

To import an LCMBIAR file, complete the following steps:

1. Launch the promotion management tool.
2. In the *Promotion Jobs* home page, click *Import* > *Import file*.
   The *Import from file* window is displayed.
3. You can import a BIAR file from the file system or from an FTP server.
   - To import a BIAR file from the file system, perform the following steps :
     1. Select *file system*.
     2. Click *Browse* and select an LCMBIAR file from the file system.
     3. In the *Password* field, enter the password of the LCMBIAR file.

        > **Note**
        >
        > The Password field is displayed only if the LCMBIAR file is encrypted with a password.

     4. Click *Create*. The job is created.

        > **Note**
        >
        > If a job with the same name exists, the Confirm Save popup is displayed. Click 'Yes' to overwrite the existing job; Click 'No' to create a job with a new name `jobname_copy<CURRENT_DATE_AND_TIME>`
   - To import an LCMBIAR file from an FTP server, complete the following steps:
     1. Select *FTP*.
     2. Enter appropriate details in the host, port, username, password, directory, and filename fields and click *OK*.

     > **Note**
     >
     > You can import only LCMBIAR files or upgrade management tool BIAR files.
4. Click *Promote*.
   The *Promote - Job Name* window is displayed.
5. From the *Destination* drop-down list, select the destination system. If you select *Login to a New CMS*, you will be prompted for credentials. Confirm the login credentials of the destination system.
6. Click *Promote* to promote the contents to the destination system.

   You can also click the *Test Promote* option to view the objects to be promoted and the promotion status.

Related Information

To manage the dependencies of a job [page 491]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.3.11 To schedule a job promotion

This section describes how to schedule the promotion of a job. It also describes how to specify the recurrence options and parameters.

To schedule the promotion of a job instance, complete the following steps:

1. In the *Promote* dialog box, click the *Schedule* option.
2. Set the required schedule option and click *Schedule*.

If you add InfoObjects to a folder contained in a job after the job has been scheduled for promotion, they will also be promoted to the destination at the scheduled time.

> **Tip**
>
> After the promotion of a job is complete, you can view all instances of the job by selecting the job on the *Promotion Jobs* page and clicking *History* on the toolbar.

Promotion of a job can also happen based on event triggers.

You can select email notifications based on job promotion status (like success/partial success/failed). For detailed information on the various scheduling options and configuring your notifications, refer to the Scheduling section.

Related Information

Exporting a job to an LCMBIAR File [page 495]

15.3.11.1 To update the recurring and pending job promotion instances

The promotion management tool allows you to track the status of and reschedule promotion job instances using the *Recurring and Pending Instances* option.

To track the statys of and reschedule promotion job instances, complete the following steps:

1. Launch the promotion management tool.
2. In the *Promotion Jobs* home page, select a job.
3. Click *History*.
   The *Job History* window is displayed.
4. Click *Recurring & Pending Instances*.
   The *Job History for Recurring and Pending Instances* window is displayed. This window displays the list of recurring and pending promotion job instances.

   You can use the following options, as necessary:

   - Click *Promoted Instances* to view the list of promoted job instances.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Click the *Pause* option to pause the selected pending or recurring instance.
- Click the *Resume* option to resume the paused scheduled promotion job instance.
- Click the *Reschedule* option to reschedule the selected promotion job instance.
- Click to delete a scheduled promotion job instance.
- Click to refresh the status of a scheduled promotion job instance.
- You can use the option to navigate a single page, or navigate to a specific page by entering the relevant page number.

> **Note**
>
> The status column in the *Job History for Recurring and Pending Instances* window displays the status of the promotion job instance, such as recurring, pending.

Related Information

To roll back a job [page 499]

15.3.12 To view the history of a job

This section describes how to view the history of a job.

> **Note**
>
> To view the history of a job, you must ensure that the status of the job is one of the following:
>
> - Success
> - Failure
> - Partial Success

To view the history of a job, complete the following steps:

1. Launch the promotion management tool.
   The *Promotion Jobs* home page is displayed.
2. Select the job for which you want to view the history, and click the *History* tab.

   The job instance time, name of the job, names of the source and destination systems, the ID of the user who promoted the job, and the status (Success, Failure, or Partial Success) of the job are displayed.

   You can view the detailed status of the job by using the link displayed in the *Status* column.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.3.13 To roll back a job

The Rollback option allows you to restore the destination system to its previous state, after a job is promoted.

To roll back a job, complete the following steps:

1. Launch the promotion management tool.
   The *Promotion Jobs* home page is displayed.
2. Perform any of the following operations:
   - Right-click the job you want to roll back, and select *Rollback*.
   - Select the job you want to roll back, and click the *Rollback* tab.

   The *Rollback* window is displayed.
3. Select the instance you want to roll back, and click *Complete Rollback*.
   The instance is rolled back.

You can roll back only the most recent instance of a promotion job. You cannot roll back multiple job instances simultaneously.

15.3.13.1 To use the Partial Rollback option

The promotion management tool allows you to roll back infoobjects in a job either completely or partially from the destination system.

To roll back infoobjects partially, complete the following steps:

1. Launch the promotion management tool.
   The *Promotion Jobs* home page is displayed.
2. Perform any of the following operations:
   - Right-click the job you want to rollback, and select *Rollback*.
   - Select the job you want to rollback, and click the *Rollback* tab.

   The *Rollback* window is displayed.
3. Select the instance from the list, and click *Partial Rollback*.

   The list of infoobjects in the selected job is displayed in the *Job Viewer* page.
4. Select the infoobjects that you want to roll back, and click *Rollback*.

> **Note**
>
> You must ensure that you have rolled back all the infoobjects in an instance before you roll back infoobjects in the next instance.

> **Caution**
>
> If a job is promoted with security, then, during the partial rollback of infoobjects, the selected dependent infoobjects may not have their security rolled back to their previous states.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To manage different versions of BI resources [page 528]

15.3.13.2 To roll back a job after the password expires

This section describes how to roll back a job, after the password that was used to promote it expires.

To roll back a job after the password expires, complete the following steps:

1. Select the job that you want to roll back, and click *Rollback*.
2. In the *Rollback* window, select *Complete Rollback*.
   An error message is displayed. This message states that the job cannot be rolled back. You are also prompted to log into the source or destination system.
3. Enter the new login credentials, and click *Login*.

A dialog box is displayed indicating that the rollback process is complete.

> **Note**
>
> The jobs that were promoted using the source or destination system credentials are updated automatically.

Related Information

To partially roll back infoobjects after the password expires [page 500]
To use the Partial Rollback option [page 499]

15.3.13.2.1 To partially roll back infoobjects after the password expires

This section describes how to partially roll back infoobjects, after the password for the source or destination system expires.

To partially roll back infoobjects after the password expires, complete the following steps:

1. Select the job that you want to roll back, and click *Rollback*.
   The *Rollback* window is displayed.
2. Select the *Partial Rollback* option.
   An error message is displayed. This message states that the infoobjects cannot be rolled back. You are also prompted to log into the source or destination system.
3. Enter the new login credentials, and click *Login*.
   The *Job Viewer* page is displayed. This page displays the list of infoobjects.
4. Select the required infoobjects, and click *Rollback*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The jobs that were promoted using the source or destination system credentials are updated automatically.

Related Information

To roll back a job [page 499]
To use the Partial Rollback option [page 499]
To roll back a job after the password expires [page 500]

15.4 To manage different versions of an infoobject

The version management application allows you to manage versions of BI resources that exist in the BI platform repository. It supports both Subversion and ClearCase version management systems. This section describes how to use the Version Management feature in the promotion management tool.

To create and manage different versions of an infoobject, complete the following steps:

1. Launch the promotion management tool.
2. Right-click a job, select *VMS Actions*, and click *Add to VM*. (You can also click the *VMS Actions* tab and then click *Add to VM*.)

   > **Note**
   >
   > Clicking *Add to VM* results in the creation of a base version of the object in the VMS repository. A base version is required for subsequent check-in.

3. Click *Checkin* to update the document that exists in the VMS repository.
   The *Check-in Comments* dialog box is displayed.
4. Enter your comments, and click *OK*.
   The change in the version number of the selected infoobject is displayed in the VMS and Content Management System columns.
5. To obtain the latest version of the document from the VMS, select the required infoobject, and click *Get latest Version*.
6. To create a copy of the latest version, click *Create Copy*.
   A copy of the selected version is created.
7. Select *History* to view all the versions available for the selected resource.
   The *History* window is displayed. The following options are displayed:
   - *Get Version* - If there are multiple versions, and if you require a particular version of the BI resource, then you can select the required resource and click *Get Version*.
   - *Get Copy of Version* - This option allows you to obtain a copy of the selected version.
   - *Export Copy of Version* - This option allows you to obtain a copy of the selected version and save it to your local system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.4.1 Version Management application access rights

This section describes the application access rights for the version management application.

- You can set access rights to the version management application within the CMC.
- You can set granular application rights to various functions within the version management application.

To set specific rights in the version management application, complete the following steps:

1. Log into CMC and select *Applications*.
2. Double-click *Version Management*.
3. Click *User Security*, and select a user. You can view or assign security rights for the selected user.
4. The following version management specific rights are now available:
    - Allow Checkin
    - Allow Create Copy
    - Allow Delete Revision
    - Allow Get Revision
    - Allow Lock and Unlock
    - View and Version BOMM objects
    - View and Version Business Views
    - View and Version Calenders
    - View and Version Connections
    - View and Version Profiles
    - View and Version QaaWS
    - View and Version Report Objects
    - View and Version Security Objects
    - View and Version Universes
    - View Deleted Resources
5. If you wish to assign rights to a selected user, select the appropriate right and click *Assign Security*.

15.4.2 Backing up and restoring Subversion files

This section describes suggested procedures to perform backups and recover Subversion files.A backup and recovery plan consists of precautions to be taken in the event of a system failure due to a natural disaster or a catastrophic event.

15.4.2.1 To back up Subversion files

Perform the following steps to backup the Subversion files:

1. On Windows, go to **<INSTALLDIR>**`\SAP BusinessObjects Enterprise 4.0\CheckOut` or in Unix, go to **<INSTALLDIR>**`/sap_bobj/enterprise_40/Subversion/CheckOut`
2. Copy the `CheckOut` folder and store it on any backup device.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Copy the entire **<LCM_Repository>** and store it on any backup device.

15.4.2.2 To restore Subversion files

Perform the following steps to restore Subversion files:

1. Restore the CheckOut folder from the earlier backed up location.

   > **Note**
   >
   > In CMC, click *Applications* > *Version Management* > *VMS Settings*, and ensure that the correct check out path is entered in the *Workspace Directory* field.

2. Restore the LCM_Repository from the earlier backed up location.

   > **Note**
   >
   > In CMC, click *Applications* > *Version Management* > *VMS Settings*, and ensure that the correct check out path is entered in the *Install Path* field.

15.5 Promoting full repository content using the promotion management tool

Promoting the contents of a repository requires planning, preparation, and sufficient time. This section describes the actions required for a successful promotion of content from one deployment to another.

15.5.1 To prepare the source and target systems

You must ensure that the source and target systems are configured optimally before promoting content.

1. On the source system:
   a. Use the Repository Diagnostic Tool (RDT) to scan and fix the source system and correct any repository or FRS inconsistencies. For more information on the RDT, see the *Business Intelligence Platform Repository Diagnostic Tool User Guide*.
   b. Minimize system usage on the source system to ensure minimal changes during promotion. An active system can result in object failure.

      > **Note**
      >
      > If failures occur, review the job status to rectify any issues.

2. On the target system:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

a. Use the license keycode to ensure that the correct and sufficient license is set on the target system.

> **Note**
>
> To avoid content promotion failure due to insufficient licensing, use identical licensing on both systems.

b. If you use third-party authentication, you must configure and enable it on the target system prior to promoting content.

> **Note**
>
> Do not map users or user groups. This will result in the creation of users or user groups with different CUIDs on the target system. The promotion process uses CUIDs to identify and map objects between the source and target system. Mapping users and user groups will cause content mismatches and will result in promotion failure.

c. Ensure that all required add-ons on the source system are also installed on the target system.

> **Note**
>
> To ensure successful migration, you must install add-ons such as Analysis or Design Studio on the source system.

d. If you have content that uses QaaWS connections, you must enable the overrides to ensure that these connections point to the correct web services. For more information on setting up overrides, see the "Overrides" section.

e. If you need to migrate all completed scheduled instances, you must click *Show completed instances in Manage Dependencies page* in the *Job Settings* of Promotion Management.

3. On the central system:

a. You can designate the source syste, the target system, or a separate system as the central system, where the Promotion Management jobs are executed. When promoting a full repository, you will handle a large amount of content that will require additional system resources on the central system. Use the following sizing reference to configure the central system for 10,000 objects:

Table 79:

	Temporary Space Allocation	Memory Allocation	Additional Configuration
`LCM_CLI`	2 GB	2 GB	Update `LCM_CLI.bat` and change the `-Xmx` parameter.
Promotion Management Job Server	3 GB	3 GB	In the CMC, update the Promotion Management Job Server start-up property by adding the `-javaargs Xmx3g` parameter.

For example, if you estimate the job to contain 50,000 objects:

- Allocate 10 GB of memory to `LCM_CLI` (50,000 ÷ 10,000 × 2)
- Allocate 15 GB of memory to the Job Server (50,000 ÷ 10,000 × 3)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> These sizing guidelines apply to most environments. However, the size of documents may affect resource requirements.

15.5.2 Migration strategies

- Use the Command-Line Interface (CLI) rather than the web CMC tool for all job promotions.
  - The CLI bypasses the twenty-minute web session limit which is involved during a promotion job that includes more than 1,000 objects.

    > **Note**
    >
    > The object limit depends on sufficient system resources.

  - The CLI provides granular control over content promotion by using query language to select the content to be migrated. You can select content of the same type or content located in the same directory.
  - The CLI can be run in batches and promotion jobs can be initiated by other scripting tools.
- Establish security by promoting the principals (users and user groups) first.
  - Promoting the users and user groups first preserves the security model on the target system and ensures the success of subsequent migration of the users' personal content (such as inboxes, favorites, and personal categories).

    > **Note**
    >
    > It is important that you perform this task first so that the CUIDs of the users and user groups on the target system will be identical to those on the source system.

- Turn off dependency calculation.
  - Dependency calculation is one of the most intensive tasks in the job creation process. During full repository migration, all objects are migrated, making the calculation unnecessary.

    > **Note**
    >
    > This feature is useful only when you are unsure of which dependent objects are required.

- Avoid including security calculation whenever possible.
  - Security calculation is the second-most intensive task in the job creation process. Break up the promotion into two jobs if you have many documents in different directories, and security is set only on the directories. The first job should contain only objects with security enabled and the second job should contain only documents with security disabled. In this manner, you can perform security calcuations only on the directories, avoiding calculating security on all documents.

    > **Note**
    >
    > Object security is preserved because it is inherited from folder security.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.6 Full system promotion steps

A full system promotion requires the execution of three separate promotion jobs in order, each promoting specific content types. The following table outlines the content types and parameter settings for each promotion job.

Promotion Job	Content Type	`exportDependencies`	`includeSecurity`
1	All users and user groups	false	true
2	All dependent objects	false	true
3	All primary objects	false	true

Use the Command-Line Interface (CLI) to create and execute each job. For more information on the CLI, see the "Using the Command Line option" section.

Common Parameters

USe the following parameters for all three promotion jobs:

> **Remember**
>
> Ensure that each parameter is on a new line.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

15.6.1 To promote users and user groups (Job 1)

To establish identical security models between the source and target systems and to ensure that the user and user groups objects' CUIDs are identical, promote the users and user groups first.

1. Create a the `usersandgroups.properties` file with the common parameters and append the following parameters to the file in order to select all users and user groups:

```
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
(SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2, 3))
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. To execute the job, navigate to **<INSTALLDIR>**\win64x64\scripts directory and run the following command:

```
Lcm_cli.bat -lcmproperties=usersandgroups.properties
```

15.6.2 To promote dependent objects (Job 2)

Dependent objects are depended upon by the primary objects in the Public folder and the users' Favorites folder. To eliminate the need to set `includeDependencies` to `true` for all other jobs, promote the dependent objects second. The following are dependent objects:

- Access Levels
- Applications
- BusinessViews
- Calendars
- Categories
- Connections
- Events
- OLAP Connections
- Profiles
- Projects
- QaaWS
- Remote connections
- Replication lists
- Server Groups
- Universes

1. Create the dependencies.properties file with the common parameters and append the following parameters to the file in order to select all dependent objects:

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target and
set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and si_specific_kind !
= 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. To execute the job, navigate to **<INSTALLDIR>**`\win64x64\scripts` directory and run the following command:

```
Lcm_cli.bat -lcmproperties=dependencies.properties
```

15.6.3 To promote primary objects (Job 3)

Primary objects are core BI documents that reside in the Public folder and the users' Favorites folder. Assuming that the second promotion job has already been executed, migrating all the dependent objects, promoting primary objects last re-establishes their relationships with dependent objects.

1. Create a the `primaryobjects.properties` file with the common parameters and append the following parameters to the file in order to select all users and user groups:

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. To execute the job, navigate to **<INSTALLDIR>**\win64x64\scripts directory and run the following command:

```
Lcm_cli.bat -lcmproperties=primaryobjects.properties
```

> **Note**
>
> If there are more than 50,000 objects in the Public folder or the users' Favorites folders, it may be necessary to break this final job into smaller jobs.

> **Note**
>
> Ensure that the machines running the Command-Line interface command and the Promotion Management Job Server both meet the sizing requirements. For more information, see the “Sizing” section.

15.6.4 Post-promotion

Promotion Management promotes only the server groups, but not their servers. To ensure that reports with designated servers will continue to work, you must recreate and assign the servers to the correct server groups.

15.7 Using the Command Line option

The command line option of the promotion management tool allows promoting objects from one BI platform deployment to another. You can create a batch script for multiple jobs.

> **Tip**
>
> Use the command line option for jobs that contain a large number of objects.

The promotion management tool supports the following job promotion types from the command line:

- Export an existing promotion job template to LCMBIAR with password encryption
- Export an existing promotion job template to LCMBIAR without password encryption
- Export single or multiple platform queries
- Promote multiple platform queries
- Promote with an existing job template
- Import and promote an existing LCMBIAR file
- Perform Live-to-Live promotion

15.7.1 To run the command-line tool on Windows

To run the command line tool, complete the following steps:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Launch a command line window or shell.
2. Navigate to the appropriate directory.

   For example, the directory path for windows is `-C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Do one of the following:
   - Execute the LCMCLI, ensure the java path is set prior to running the program.
     Command: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <property file>`
   - Run the BAT file from `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat`
     Command: `lcm_cli.bat -lcmproperty <property file>`

   > **Note**
   >
   > Enter the valid passwords when prompted.

The promotion management command line tool takes a **<properties>** file as a parameter. The **<properties>** file contains the required parameters to communicate with the promotion management tool about the actions to perform, connection to which BI platform deployment, connection methods, objects to promote.

The file must be in the form of **<FILENAME>**`.properties`

For Example: **<Myproperties.properties>**

15.7.2 To run the command-line tool on Unix

To run the command line tool, complete the following steps:

1. Launch shell.
2. Navigate to the appropriate directory.

   For example, `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib`
3. Do one of the following:
   - Execute the LCMCLI, ensure the java path is set prior to running the program.
     Command: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <property file>`
   - Run the BAT file from `<installdir_path>\sap_bobj\lcm_cli.sh`
     Command: `lcm_cli.sh -lcmproperty <property file>`

   > **Note**
   >
   > Enter the valid passwords when prompted.

15.7.3 Command-line tool parameters

The following table describes the parameters and the allowed values for the command line option of the promotion management tool.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Remember

Do not place command-line parameters within quotation marks.

Table 80:

Parameter	Allowed Values	Description	Mandatory vs Optional
`action`	Export, Promote Example: `action=export`	This option allows you to specify the operation that the CLI must perform. This operation can perform any of the following operations: • Promote objects from an LCMBIAR file or a promotion management job to a BI platform system. • Export objects from a BI platform system to an LCMBIAR file.	Mandatory
`consolelog`	true or false	This parameter is used to display the complete log of the command executed by the user in the command log.	Optional If not specified the default is false.
`Destination_authentication`	secEnterprise, secWinAD, secLDAP,secSAPR3 Example: `Destination_authentication=<authentication>`	This parameter indicates the authentication type to be used.	Optional If the authentication type is not specified, `secEnterprise` is used
`Destination_clientID`	Client ID Example: `Destination_clientID=<systemID>`	This parameter is used for SAP authentication only.	Mandatory for SAP authentication.
`Destination_CMS`	Free form text. Example: `Destination_CMS=<CMSname: port no.>`	This parameter enables the user to specify the CMS to which the tool must connect.	Mandatory if `action=promote`
`Destination_password`	Free form text. Example: `Destination_password=<password>`	This parameter specifies the associated password of the user account.	Mandatory if `action=promote`
`Destination_systemID`	System ID Example: `Destination_systemID=<systemID>`	This parameter is used for SAP authentication only.	Mandatory for SAP authentication.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Allowed Values	Description	Mandatory vs Optional
`Destination_userName`	Free form text. Example: `Destination_username=<username>`	This parameter specifies the user account that the tool must use to connect to the BI Platform CMS. **Note** Delegated administrator is supported.	Mandatory if `action=promote`
`exportLocation`	Free form text. Must have **`<.lcmbiar>`** extension Example: `exportLocation=C:/Backup/New.lcmbiar`	This parameter enables the user to specify the location to place the LCMBIAR file after the objects have been exported and packaged.	Mandatory if `action=export`
`exportDependencies`	false, true Example: `exportDependencies=<true or false>`	This parameter specifies the object dependencies that the tool gathers for exportation. It is applicable only when used in conjunction with the `Source_CMS` flag.	Optional, used if `action=promote or export` If not specified the default is false.
`exportQuery`	Free form text. Use the CMS query language format. Example: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi` **Note** You can have any number of queries in one properties file, but they must be named as exportQuery1, exportQuery2.	These are the queries the tool should execute to gather the desired objects for exportation.	Optional, used if `action=promote or export`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Allowed Values	Description	Mandatory vs Optional
`exportQueriesTotal`	Positive whole numbers`exportQueriesTotal=<whole number>`	This parameter enables the user to specify the number of export queries to execute. If you have x export queries and want to execute them all, you must set this parameter value to x.	Optional, used if `action=promote or export` If not specified, default equals 1
`importLocation`	Free form text. Must have **`<.lcmbiar>`** extension Example: `importLocation=C:/Backup/New.lcmbiar`	This parameter enables the user to specify the location of the LCMBIAR file that contains the objects to be promoted.	Optional if `action=promote`
`includeApplicationSecurity`	false, true Example: `includeApplicationSecurity=<true or false>`	This parameter instructs the tool to export or import the security associated with selected applications.	Optional, if not specified the default is false. Used if `action=promote or export`
`includeSecurity`	false, true Example: `includeSecurity=<true or false>`	This parameter instructs the tool to export or import the security associated with selected objects and selected users. If access levels are used this will also export/import them.	Optional, if not specified the default is false. Used if `action=promote or export`
`JOB_CUID`	The CUID of the saved Promotion Management job.	This parameter instructs the tool to export all the objects in the job to the LCMBIAR file.	Optional, used if `action=export or promote`
`lcmbiarpassword`	Free form text Example: `java -cp lcm.jar com.businessobjects.lcm.cli.LCMCLI -lcmproperty lcm.properties -lcmbiarpassword "<testpassword>"`	This parameter enables the encryption and decryption of BIAR files using a password .	Optional,if not specified or if the string is empty, implies there is no encryption

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Allowed Values	Description	Mandatory vs Optional
`lcmproperty`	The full path of the location where property file has been saved `lcm_cli.bat -lcmproperty <file path of the property file>`	This parameter refers to the values required for the execution of a command, which are saved in a file.	Mandatory
`limitQueryBatchSize`	false, true Example: `limitQueryBatchSize=<true or false>`	This parameter restricts the number of returned objects to 1,000 by default. When this parameter is set to false, all queried objects will be returned. **Note** You can also explicitly set the new limit for the number of objects returned by the query using `select TOP <number>`	Optional, if not specified, default equals true
`LCM_authentication`	secEnterprise, secWinAD, secLDAP,secSAPR3 Example: `LCM_authentication=<authentication>`	This parameter indicates the authentication type to be used.	Optional. If the authentication type is not specified, `secEnterprise` is used
`LCM_clientID`	Client ID Example: `LCM_clientID=<clientID>`	This parameter is used for SAP authentication.	Mandatory for SAP authentication.
`LCM_CMS`	Free form text. Example: `LCM_CMS=<CMSname:portno.>`	This parameter enables the user to specify the CMS for the promotion management tool.	Mandatory if `action=promote or export`
`LCM_password`	Free form text. Example: `LCM_password=<password>`	This parameter enables the user to specify the password of the user account.	Mandatory if `action=promote or export`
`LCM_systemID`	System ID Example: `LCM_systemID=<systemID>`	This parameter is used for SAP authentication.	Mandatory for SAP authentication.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Allowed Values	Description	Mandatory vs Optional
`LCM_userName`	Free form text. Example: `LCM_userName=<username>`	This parameter enables the user to specify the account username that the tool must use to connect to the promotion management tool CMS. **Note** Delegated administrator is supported	Mandatory if `action=promote or export`
`Source_authentication`	secEnterprise, secWinAD, secLDAP,secSAPR3 Example: `Source_authentication=<authentication>`	This parameter indicates the authentication type to be used.	Optional. If the authentication type is not specified, `secEnterprise` is used
`Source_clientID`	SAP Client ID Example: `Source_clientID=<systemID>`	This parameter is used for SAP authentication only.	Mandatory for SAP authentication.
`Source_CMS`	Free form text. Example: `Source_CMS=<CMSname:port no.>`	This parameter enables the user to specify the CMS to which the tool must connect.	Mandatory if `action=export`
`Source_password`	Free form text. Example: `Source_password=<password>`	This parameter specifies the associated password of the user account.	Mandatory if `action=export`
`Source_systemID`	SAP System ID Example: `Source_systemID=<systemID>`	This parameter is used for SAP authentication only.	Mandatory for SAP authentication.
`Source_userName`	Free form text. Example: `Source_username=<username>`	This parameter specifies the user account that the tool must use to connect to the BI platform CMS. **Note** Delegated administrator is supported.	Mandatory if `action=export`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Allowed Values	Description	Mandatory vs Optional
`stacktrace`	true or false Example: `stacktrace=<true or false>`	This parameter enables the user to trace all calls.	Optional, if not specified, default equals false

Note

- Similar to the creation of a job before exporting, the Command Line option creates a temporary job on the fly. This job name could be a combination of `Query_<USER>_<Timestamp>`. This is specific only to **`<exportQuery>`**.
- You can rollback the job only through the promotion management tool. There is no command line support to rollback the jobs.
- When working with a large number of objects, it is recommended to increase the maximum Java heap size by setting the `-Xmx=8g` parameter in the `LCMCLI` script.

15.7.4 Sample properties file

The following is a sample `properties` file:

Example

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<CMS name:port number>
LCM_userName=<username>
LCM_password=<password>
LCM_authentication=<authentication>
LCM_systemID=<ID>
LCM_clientID=<client ID>
Destination_CMS=<CMS name:port number>
Destination_userName=<username>
Destination_password=<password>
Destination_authentication=<authentication>
Destination_systemID=<ID>
Destination_clientID=<client ID>
lcmbiarpassword=<password>
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> If the `properties` file does not have any personal information, the LCM CLI will prompt for the same in the console.

15.8 Using the Enhanced Change and Transport System

The Change and Transport System (CTS) organizes and customizes development projects in the ABAP Workbench, and then transports these changes between SAP Systems in your system landscape. The Enhanced Change and Transport System (CTS+) is an add-on to the CTS that promotes non ABAP content across CTS+ enabled non-ABAP repositories.

BI platform infoobjects can use SAP Business Warehouse content as a data source. The integration of CTS+ with the promotion management tool enables the handling of the BI platform repository, in a similar way to the SAP Business Warehouse (BW) repository, by using CTS transport requests to promote jobs. CTS+ provides an option to transport non-SAP objects within a system landscape. For example, objects created in the development system can be attached to a transport request and forwarded to other systems within the landscape.

For more information about the Change and Transport System, see Change and Transport System - Overview (BC-CTS)

For more information about CTS+ and non ABAP transports, see Transporting Non-ABAP Objects in Change and Transport System

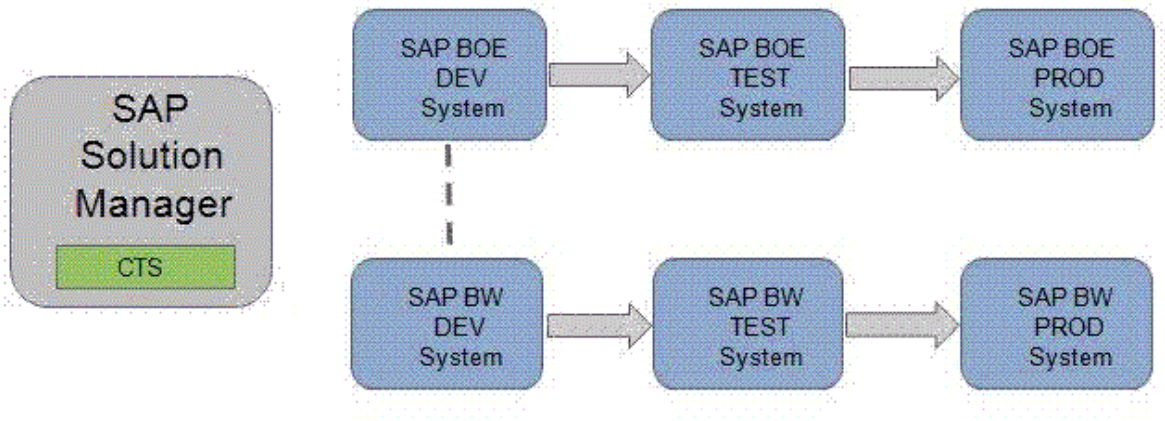
15.8.1 Prerequisites

The following are the prerequisites for transporting business intelligence content from system to another through CTS+:

1. BI platform 4.0 (or newer) is installed.
2. SAP Solution Manager 7.1 or SAP Solution Manager 7.0 EHP1 (minimum SP25) is installed and is used as the domain controller for CTS+, at least for the configuration of SAP BusinessObjects systems.
   For more information about configuring the transport domain, see Configuring the Transport Domain.
3. The CTS plug-in is installed on the SAP Solution Manager (CTS plug-in is taken from SL Toolset 1.0 SP02. We recommend that you use the latest available CTS plug-in).
   For more information on installing the required CTS plug-in, see the SAP Note: SAP Note 1533059.
4. *SAP Business Warehouse 7.0* (SPS 24 or higher) systems are installed. For more information, see SAP note SAP Note 1369301.
5. SAP Business Warehouse (SAP BW) transport landscape is configured in the Change and Transport System (CTS).
6. SAP Note 1692417 and SAP Note 1860594 have been implemented on the machine that hosts the CTS Deploy Web Service.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.8.2 To configure the BI platform and CTS+ Integration



The Transport Management System (TMS) which is part of the Change and Transport System is used to transport changes between the SAP systems within a landscape. It manages the connected systems, their routes, and the imports into its systems. For more information about the Transport Management System, see Transport Management System (BC-CTS-TMS)

CTS+ enables collection of files from outside and their distribution within a transport landscape. The Transport Organizer Web UI, which is part of CTS+, manages the transport requests and the objects contained by it. For more information, see Transport Management System (BC-CTS-TMS)

You can integrate BI platform promotion management with CTS+ and SAP BW using CTS transport requests.

> **Note**
>
> To enable the integration of the BI platform with SAP Solution Manager, you need to define "BOLM" application type in the SAP Solution Manager landscape.

Perform the following steps to integrate the BI platform and CTS+:

1. Activate the CTS export web service.
2. Configure CTS settings in the promotion management tool.
3. Configure the BI platform import system in SAP Solution Manager.

Related Information

To activate the CTS Export web service [page 519]
To configure CTS+ settings in the promotion management tool [page 519]
To configure the BI platform and CTS+ Integration [page 518]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.8.2.1 To activate the CTS Export web service

To configure BI platform, you need activate CTS export web service in the SOA Management web tool.

1. To start the application, enter the transaction code SOAMANAGER in your SAP Solution Manager. After the required authentication is done, the SOA Management Console opens in a Web browser.

   For more information on SOA Management and the configuration of a service endpoint using SAP Solution Manager 7.0, see Configuring a Service Provider. For SAP Solution Manager 7.1, see Configuring a Service Provider.
2. On the *Application and Scenario Communication* tab, click *Single Service Configuration*.

   The CTS Export Web Service is named `EXPORT_CTS_WS`
3. In the *Configuration* tab, create or edit the service endpoint.
4. In the *Security* tab, configure the transport protocol and authentication method.
5. In the *Transport Settings* tab, define alternative access URL for the convenient access of the service endpoint.

15.8.2.2 To configure CTS+ settings in the promotion management tool

The following section describes the configuration steps to be performed in the CMC application to set up CTS+ for usage with the promotion management tool.

1. In the *Promotion Jobs* page, click *CTS Settings* and then click *BW Systems*.
2. In the *BW Systems* page, click *Add* to add a BW system to the landscape.
3. In the *Add System* page, enter the following details:
   - *Host BW SID* : specify the system ID (SID) of the host SAP BW/ABAP machine.
   - *Host Name*: specify the IP address of the host machine.
   - *System number*: enter the system number of the host system.
   - *Client*: refers to the system details of the client machine.
   - *User* and *Password*: specify the user name and password on the client machine in these fields.
   - *Language*: specify your choice of language in this field.
4. Click *OK* to add the system to your landscape.

   > **Note**
   >
   > Once you've added a BW system to your landscape, you can use the *Edit* or *Delete* in the *BW Systems* page to modify the systems in your landscape.
5. In the *Promotion Jobs* page, click *CTS Settings* and then click *Web Service Settings*.
6. In the *Web Service Settings* page, enter the Web Service URL and user details.

   > **Note**
   >
   > If you're not familiar with these details, obtain the same from the Solution Manager administrator.
7. Click *Save* and *Close* to complete adding the web service settings.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

8. Create a mapping file for the BI platform promotion management CMS system.

   Complete the following steps in the BI platform development system to create a text file with connectivity details to enable the mapping:

   a. In the BI platform promotion management CMS, go to the root directory and create a folder with name **LCM** in the path **<INSTALLDIR>**/SAP BusinessObjects Enterprise XI 4.0/
   b. Create a text file with name LCM_SOURCE_CMS_SID_MAPPING.properties, and enter either one of the following in the file:
      - **<Complete name of the SAP BI platform source system with domain>@<CMS port number>** = **<logical name for source system as used in CTS configuration >**
      - **<IP number of the SAP BI platform source system>@<CMS port number>** = **<logical name for source system as used in CTS configuration >**

   For example:

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> **Note**
>
> In case of clustered environment, copy the LCM_SOURCE_CMS_SID_MAPPING.properties file to the system where Adaptive Processing Server is running.

For more information about performing configuration steps for non-ABAP systems, see Making Transport Settings in the Application.

15.8.2.3 To configure the BI platform import system in the SAP Solution Manager

1. Log on to the SAP Solution Manager system.
2. Enter transaction `stms` and press `Enter`.
3. Configure BOLM as the application type.
   a. Go to *Overview* > *Systems*.
   b. Go to *Extras* > *Application Type* > *Configure*.
   c. Choose *New Entries*.
   d. In the *Application Type* field, enter **BOLM**.
   e. Enter description.
   f. In the *Support Details* field, enter **http://service.sap.com (ACH: BOJ-BIP-DEP)**
   g. Choose *Table View* > *Save*.
   h. Confirm the prompt by choosing *Yes*.
4. To work with different languages, you can maintain translated text as follows:
   a. Choose *Goto* > *Translation*.
   b. Select the languages into which you want to translate the text.
   c. Enter the translated values in the *Description* and *Support Details* fields.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

d. Confirm the dialog box.
e. Choose *Continue*.
f. Choose *Table View* > *Save*.
g. Confirm the prompt.

The TMS domain is now ready to support usage of business intelligence content in CTS.

5. In CTS+, define the BI platform source system as an export system.

> **Note**
>
> For more information on creating a non-ABAP system as a source system, see Defining and Configuring Non-ABAP Systems

6. In CTS+, configure the BI platform import system by completing the following steps:

> **Note**
>
> You can define a SID as a reference to the BI platform import system.

a. Create a non-ABAP system as an import system.

   For more information, see Defining and Configuring Non-ABAP Systems.
b. Specify the deployment method as *Other* and deselect all other options.
c. Choose *Save*.
d. Confirm the distribution dialog box.
   The table view to configure the import system settings appears.
e. Choose *Edit* > *New Entries*.
f. In the "Change View CTS: System details for handling of application types" screen, perform the following steps:

   1. In the *Deploy Method* field, select *application specific Deployer (EJB)*.
   2. In the *Deploy URI* field, enter the following URI: **`http://<BOE web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`**
      where
      - "BOE web server name" is the name or IP address of the machine where the BI platform web server is running.
      - "Web server port" is the port number of the BI platform web server.
      - "BOE destination name" is the name of the machine on which the target BI platform Central Management Server (CMS) is running.
      - "CMS port" is the port number of the target CMS.
      - "BOE authentication type" is the type of user authentication for importing business intelligence content. The supported authentication types are secEnterprise, secLDAP, secWinAD, and secSAPR3.
   3. In the *User* field, enter the BI platform user name.
   4. In the *Password* field, enter the BI platform password.
   5. Choose *Save* to save the settings.

If you require more than one import system, repeat the steps above to create all destination systems required. To configure transport routes between the source and target system after the creation of the destination systems, see Configuring Transport Routes

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

15.8.2.4 To export from BI platform to CTS+ with SSL

15.8.2.4.1 To configure SSL for CTS+

To configure SSL for CTS+, you must configure SSL on Application Server ABAP. For more information, see Configuring the SAP Web AS for Supporting SSL.

15.8.2.4.2 To configure the client-side SSL certificate

To configure the client-side SSL certificate, you must either import the server certificate or the trusted CA certificate into the JVM keystore.

1. Back up the `cacerts` files from the **<INSTALLDIR>**`\win64_x64\sapjvm\jre\lib\security` directory.
2. Import the certificate into the Tomcat JVM that hosts the `BOE.war` file using the following parameters:

```
<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer -
keystore cacerts
```

3. Restart Tomcat.

15.8.2.4.3 To configure the CTS+ Export Web Service

To configure the HTTPS-enable CTS+ Export Web Service (`EXPORT_CTS_WS`) you can create a new HTTPS endpoint.

> **Note**
>
> Alternatively, you can switch your existing HTTP endpoint to use HTTPS.

1. Use transaction code **soamanager**, and on the *Provider Security* tab, under *Communication Security*, select *SSL over HTTP (Transport Channel Security)* and Under *Transport Channel Authentication*, select *User ID/ Password*.
2. On the *Transport settings* tab, under *Transport Binding*, select *HTTPS* for *Calculated Protocol*.

15.8.2.4.4 To configure promotion management for SSL

> **Remember**
>
> Import the server certificate or the trusted CA certification into the JVM keystore.

1. In the CMC, on the *Promotion Management* tab, click *Settings* > *CTS Settings* > *Web Service Settings*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Ensure that the *Web Service URL* parameter includes `https://` and the port number configured above.

> **Note**
>
> *Promote via CTS* will not be displayed in the *Job destination* list or in the *Overrides* dialog box if the specified URL cannot be reached. If the SSL handshake between promotion management and CTS+ fails, an error will be recorded in the CMC log file.

15.8.2.5 To import from CTS+ to BI platform with SSL

15.8.2.5.1 To configure BI platform Tomcat to use HTTPS

To configure BI platform Tomcat to use HTTPS, you must perform the following steps on the machine where BI platform is installed.

1. Create a server key pair, a certificate, and a keystore.
   a. Run **<INSTALLDIR>**`\win64_x64\sapjvm\jre\bin\keytool.exe` with the following parameters:

```
keytool -genkey -alias server -keyalg RSA -keysize 1024 -keystore
serverkeystore.jks -storetype JKS

keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
serverkeystore.jks
```

   b. When prompted, enter the following information:
      - Your first and last names
      - The name of your organizational unit
      - The name of your organization
      - The name of your city or locality
      - The name of your state or province
      - The two-letter country code for this unit

      A formatted string will be displayed (for example, `CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA`). Type **yes** and press `Enter` to confirm.
2. Send the server certificate request to a Certification Authority (CA).
3. Import the signed server certificate into the server keystore using the following parameters:

```
keytool -import -alias server -keystore serverkeystore.jks -trustcacerts -file
server.crt
```

4. Configure the Tomcat configuration file `server.xml` to enable HTTPS and to use the server keystore that you have created.
5. Restart Tomcat and test the connection by accessing the following URL in a browser: `https://` **<SERVERNAME>:<SSLPORTNUMBER>**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

To configure SSL for CTS+ [page 522]

15.8.2.5.2 To configure CTS+ for SSL

To configure CTS+ for SSL, you must create an SSL client PSE and import a certificate into it.

Related Information

To configure SSL for CTS+ [page 522]

15.8.2.5.3 To update the test and production systems in CTS+ to use HTTPS

To enable HTTPS on the test and production systems, perform the following steps:

1. Use the STMS transaction code.
2. Click *System Overview*.
3. Select your test or profuction system and click *Goto* > *Application Types* > *Deployment Method*.
4. Ensure that the *Deploy URI* parameter includes `https://` and a configured HTTPS port number.

15.8.3 To promote a job using CTS

This section describes the workflow that the promotion management tool supports for promoting BI platform Central Management Server (CMS) objects from the source system to a destination system using the Change Transport System. To use CTS to promote a job, complete the following steps:

1. Launch the promotion management tool using SAP authentication, and create a job.
   For more information on creating a new job, see the "Creating a Job" section in the related links below .

   > **Note**
   >
   > Ensure that you select "SAP" as the authentication type in the source system login screen.

2. From the *Destination* drop-down list, select the *promote via CTS* option.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. Click *Create*.
   The *Add Objects from the System* screen appears. Here the folders and subfolders are displayed in a tree structure.
4. Navigate to the folder from which you want to select the infoobject.
5. Select the infoobject that you want to add to the job, and click *Add*. If you want to add an infoobject and exit the *Add Objects* screen, click *Add and Close*.
   The infoobject is appended to the job and the *Promotion Jobs* screen appears.

   > **Note**
   >
   > On the Promotion Jobs screen you can do the following:
   >
   > - Use the *Add Objects* option to add more info objects to the job. For more information, see Adding an Infoobject to a job.
   > - Use the *Manage Dependencies* option to manage the dependencies of the info object you have selected. The SAP BW dependencies of the object are displayed on the UI and available for the user to select.
   >   For more information, see Managing Job Dependencies.

6. Click *Promote*.
   The *Promote* screen appears which displays the ID, owner and a short description of the currently set default transport request.
7. You can use the *Transport Requests* hyperlink to do the following:
   - View details of the transport request.
   - Change settings of the default transport request.
   - Choose a different transport request.
   - Create a transport request.

   1. Click the *Transport Requests* hyperlink to open the *Transport Organizer* Web User Interface.
   2. If prompted for logon credentials, log on using valid user credentials for the CTS domain controller system.
   3. Refresh the *Promote* Screen to view your updates.

   For more information about using the *Transport Organizer* Web UI, see Transport Organizer Web UI
8. To view the details of the dependencies of the SAP BW objects, click the *Second level dependencies* hyperlink.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Only the objects that are locked in a request are displayed when you click the *Second level dependencies* hyperlink. If the request has been released you can not view any dependencies. In addition, this hyperlink is grayed out if there are no active second level dependencies.

9. Click *Promote*.
10. Close the job.
    The promotion management main screen is displayed. The status of the job that you created is now *Exported to CTS*.
11. Release the BI platform object to the destination system by completing the following steps:
    a. Click the link displayed in the status column of the job that you want to promote.
       The *Promotion Status* window appears.
    b. Click *State of Request*.
       The *Transport Organizer* Web UI appears.
    c. If the status of the request is *Modifiable*, click *Release* to release the transport request of the BI platform object . For more information about releasing transport requests containing non-ABAP objects, see Releasing Transport Requests with Non-ABAP Objects
    d. Close the *Transport Organizer* Web UI.
12. To view the dependencies for the SAP BW objects, click *List of BW dependencies* hyperlink.

> **Note**
>
> We recommend talking to the SAP BW team to get updates on the SAP BW dependencies and their release as these objects are worked on by the team.

13. Close the *Promotion Status* window.
14. Import the BI platform object to the destination system by completing the following steps:
    a. Log on to the CTS+ domain controller.
    b. Call the **STMS** transaction to enter the transport management system.
    c. Click on the *Import Overview* icon.
       The *Import Overview* screen appears and you can view the import queue items from all the systems.
    d. Choose the system ID of the destination Promotion Management system.
       You can see the list of transport requests that can be imported to the system.
    e. Click *Refresh*.
    f. Import the relevant transport requests. For more information, see Importing Requests

       For general information about importing transport requests with BOLM content, see Importing Transport Requests with Non-ABAP Objects
15. If the object that you selected has SAP BW dependencies, perform the following steps:
    a. Release the SAP BW dependencies to the destination system by completing the following steps:
       1. Log on to the SAP BW source system.
       2. Call SE09 transaction. The *Transport Organizer* screen appears.
       3. Click *Display* .The SAP BW request is displayed.
       4. Click the SAP BW request and expand it to view the tasks created for the dependencies.
       5. Right click the request associated with the primary SAP BW object and select *Release Directly*.
          Repeat this step to release all the tasks associated to each dependent separately.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Right click on the request associated to the primary BW object and select *Release Directly*.
7. Refresh the screen until all the requests are released.

> **Note**
>
> You can view the logs for a request by double clicking it.

b. Import the SAP BW dependencies to the destination system by completing the following steps:

1. Log on to the SAP BW destination system.
2. Call the STMS transaction to enter the transport management system.
3. Click the *Import Overview* icon. The *Import Overview* screen appears.
4. Double-click the system ID for the SAP BW destination. You can see the list of transport requests that can be imported to the system.
5. Import the relevant transport requests. For more information, see Importing Requests
   For more information about Transports with Import Queues, see Transports with Import Queues

16. Log on to the destination system to view the status of the job you promoted.

For information on generic CTS, see Configuring Target Systems for Further Applications

Related Information

To create a job [page 486]
To manage the dependencies of a job [page 491]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

16 Version Management

16.1 To manage different versions of BI resources

The version management application allows you to maintain different versions of BI resources that exist in the BI platform repository. To facilitate this feature, the tool includes Subversion version control system.

> **Note**
>
> ClearCase is not included with the BI platform installation. To use it with Version Management, you must install it.

To manage different versions of jobs or other infoobjects, complete the following steps:

1. Log into the CMC application and select *Version Management*.
2. From the left panel of the *Version Management* window, select the folder to view the job or other infoobjects whose versions you want to manage.
3. Select the infoobjects and click *Add to VM*.

   > **Note**
   >
   > Clicking *Add to VM* results in the creation of a base version of the object in the Version Management System (VMS) repository. A base version is required for subsequent check-in.

4. On subsequent changes to the document and to version the incrementally changed document, click *Checkin*. This will update the document that exists in the VMS repository.

   The *Check-in Comments* dialog box is displayed.
5. Enter your comments, and click *OK*.
   The change in the version number of the selected infoobject is displayed in the *VMS Version* and *CMS (Central Management Server) Version* columns.
6. To obtain the latest version of the document from the VMS, select the required infoobject, and click *Get latest Version*.
   The last version from the VMS repository is imported to the CMS.
7. To create a copy of the latest version, click *Create Copy*.
   A copy of the selected version is created in the VMS and CMS repositories.
8. Select *History* to view all the versions available for the selected infoobject.
   The *History* window is displayed. The following options are displayed:
   - *Get Version* - If there are multiple versions, and if you require a particular version of the BI resource, then you can select the required infoobject and click *Get Version*.
   - *Get Copy of Version* - This option allows you to obtain a copy of the selected version.
   - *Export Copy of Version* - This option allows you to obtain a copy of the selected version and save it to your local system.
   - *Compare* - This option enables you to compare the metadata information of two versions of a job. For more information, see “Comparing different versions of the same job”.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9. Select an infoobject and click *Lock* to lock the infoobject,or *Unlock* to unlock the infoobject, or *Delete* to delete all versioned content from the VMS repository. Content in the CMS is not affected.

   > **Note**
   >
   > If you lock an infoobject, you cannot perform any action on that infoobject.

10. When the version in the CMS is newer than the version in the VMS, an indicator is displayed beside the updated infoobject. When you place the cursor on the indicator, the `The version in CMS is newer` tool tip is displayed.
11. To view the list of all checked in resources that exist in the VMS but not in the CMS, click *View Deleted resources*.
    Click any deleted resource to view the history of that resource. You can select a deleted resource, and click *Get Version* to view that particular version of the resource.

    Click *Delete* to permanently drop the object from the VMS repository as well.

    > **Note**
    >
    > If you use *Get Version*, the resource is moved from the VMS missing file list to the CMS.

12. Select an infoobject, and click to view the properties of the infoobject.
    Alternatively, you can right-click the infoobject and perform steps 3 to 12.

16.2 Starting and stopping Subversion manually on Unix

On Unix, Subversion may not start automatically after the machine is restarted. From BI platform 4.1 SP2, you can run **<INSTALLDIR>**`/svn_startup.sh` to start Subversion and **<INSTALLDIR>**`/svn_shutdown.sh` to stop it.

> **Note**
>
> `svn_shutdown.sh` will work only if `svnserve` is started using `svn_startup.sh`

> **Restriction**
>
> If the Subversion process is running before the SP2 patch installation, `svn_shutdown.sh` will not work after the patch is installed. To restart Subversion, you must manually terminate the `svnserve` process and then run `svn_startup.sh`.

16.3 Required files for Subversion on Solaris 10 and RedHat Linux 5

The following files are required to run Subversion.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> If any of the following binaries are not present prior to installation of BI platform 4.1 SP1, the user must run **<INSTALLDIR>**/sap_bobj/lcm_installer.sh **<SUBVERSION_PASSWORD>** **<CMS_PASSWORD>** and then restart the Adaptive Processing Server in order for Version Management to function correctly.

- On Solaris 10, you must install the `CSWlibiconv2` and `CSWlibgcc-s1` packages that contain `libiconv.so.2` and `libgcc_s.so.1`

  > **Remember**
  >
  > After installing the packages, ensure that the path to these libraries is included in the user's `LD_LIBRARY_PATH` environment variable.

- On RedHat Linux 5, you must deploy `libexpat.so.1`

16.4 To use the Version Management System settings option

You can set the Version Management System settings and configure the Subversion and the ClearCase parameters from the Central Management Console.

1. In the CMC, click *Applications*.
2. Double click *VMS*.
   The Version Management Settings screen is displayed.
3. Select *VMS Settings*.
4. From the *Version Management Systems* list, select *Subversion*.
   The server port number, password, repository name, server name, user name, the name of the workspace directory and the name of the installation path (that were provided during the promotion management tool installation process) are displayed in the appropriate fields.
5. Modify the fields as required.

   > **Note**
   >
   > Ensure that you enter the install path that contains the `.exe` file.

   On Windows: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\Subversion`

   On Unix: **<INSTALLDIR>**`/sap_bobj/enterprise_40/subversion/bin`
6. Select *SVN*, *HTTP*, or *HTTPS*.

   > **Note**
   >
   > For more information on connecting to Subversion using HTTPS see the *Apache Subversion Documentation*.
7. (Optional) Click *Test VMS* to validate your VMS settings.
8. Click *Save*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> - If you want Subversion to be your default VMS, select *Use as Default VMS*.
> - If you have modified the fields, restart the Adaptive Processing Server.

16.4.1 Default Version Management System settings

When the CMS is reinitialized, all application settings are erased. The following are the default settings of the Version Management System:

Table 81:

Parameter	Value
Server Name	`localhost`
Server Port	`3690`
User Name	`LCM`
Password	Entered during installation.
Installation Path	On Windows: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\Subversion` On Unix: **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/subversion/bin`
Repository Name	On Windows: `svn_repository` On Unix: `LCM_repository`
Workspace Directory	On Windows: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\CheckOut` On Unix: **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/CheckOut`
Protocol	`SVN`

16.4.2 To set the ClearCase Version Management System in Windows

To set the ClearCase version management system in Windows, complete the following steps:

1. In the *Administration Options* window, click *VMS Settings*.
2. From the *Version Management Systems* drop-down list, select *ClearCase*.
3. Enter the following details:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- ClearCase Map Drive - Enter the drive name. By default, it is the M drive. For example: `M:`
- VOB Tag Name - Enter the Versioned Object Base (VOB) name. For example: FridayVB
- View Storage Directory - Enter the path to the shared folder. For example: `\\HostName\FolderName`

> **Note**
>
> The host name must not be written as localhost.

4. Click *Save*.
5. To use ClearCase as the default Version Management System, select *Use as Default VMS*.

16.4.3 To set the ClearCase Version Management System in Unix

To set the ClearCase version management system in Unix, complete the following steps:

1. In the Administration Options window, click *VMS Settings*.
2. From the Version Management Systems drop-down list, select *ClearCase*.
3. Enter the following details:
   - ClearCase Map Drive - Enter the name of the folder where the MVFS is located. By default, it is `/view`
   - VOB Tag Name - Enter the VOB name and the folder where the VOB is located. For example: `VobFolder/VobName`
   - View Storage Directory: Enter the path of the directory where the views are created.
4. Click *Save*.
5. To use ClearCase as the default Version Management System, select *Use as Default VMS*.

16.5 To compare different versions of the same job

You can view the differences between two versions of the same job by completing the following steps:

1. Log into the CMC application.
2. From the CMC home page, select *Version Management*.
3. From the Version management screen, select the job whose versions needs to be compared.
4. Click *History*.
   The History page appears which displays all the versions of the selected infoobject.
5. Select any two versions for comparison.
6. Click *Compare*.
   The comparison process starts and the differences are highlighted in orange color, and the missing objects are highlighted in red color.
7. Click *Save* to save the difference report.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

16.6 To upgrade Subversion content

If you have old Subversion content that was created using a previous version of the BI platform, you can upgrade your content to the latest version by following these steps:

1. Log on to the VMS on the SAP BusinessObjects Enterprise 3.x machine.
2. Check-in any object. For example, check in the administrator and guest objects twice.
3. In CMC, click *Users* and verify that `2` is displayed in the in VMS and CMS version number.
4. Log off from the VMS.
5. Go to the command prompt, navigate to `C:\Program Files\Subversion\bin`, and run the export command: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Copy the `dumrepo` file to the BI platform machine
7. Go to the command prompt on the BI platform machine, navigate to `C:\Program Files (x86)\SAP`, and execute the following commands:

   ```
   svnadmin.exe load "C:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
   ```
8. After the commands have been successfully executed, restart the SIA.
9. Login to the CMC and click *Version management*.
10. Click on *Users*, and verify that the VMS version is `2`.
11. Select the *Administrator* object and then click *Get Latest Version*.
12. The version number on the VMS and CMS are now the same.

16.7 Configuring Subversion for clustered Processing Job Servers

16.7.1 Option A: To configure the main Subversion machine before any Version Management System operations

1. Verify that the working copy directory has not been created at **<INSTALLDIR>**`\CheckOut`
2. Create a directory for your Subversion working copy files and share it, making it writeable from other machines.
3. In the CMC, on the Version Management System settings page, change the *Server Name* from **localhost** to the address of your main machine.
4. Change the *Workspace Directory* to your working copy share, in the following format: `\\`**<HOSTNAME>** `\`**<SHARENAME>**
5. Stop the Server Intelligence Agent (SIA) and change the account from LocalSystem to the operating system administrator.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> LocalSystem does not have network access to the shared directory.

6. Start the SIA.

> **Note**
>
> If the SIA has already been running under an account with network access to the shared directory, you only need to restart all the Processing Job Servers that host the Version Management System for steps 3 and 4 to take effect.

16.7.2 Option B: To configure Subversion after the Version Management System creates a working copy directory

1. Verify that Subversion has been installed as part of the BI platform.
2. Share the working copy directory located at **<INSTALLDIR>**\CheckOut and make it writeable from other machines.
3. Establish the name of the workspace using one of the following methods:
   - Perform a Version Management System (VMS) operation using the main machine. Then, inspect the Subversion working copy directory to determine the name of the workspace.
   - Calculate the name of the workspace by removing the symbol @ and replacing all colons with the character *B*. For example, if the cluster is named ABCD-LCM:6400, the VMS will use ABCD-LCMB6400 as the workspace name.

> **Note**
>
> Subversion stores its repository in the working copy directory.

4. Change the default URL from **localhost** to one that any machine can use by running the following command:

```
svn switch --relocate svn://localhost:3690/svn_repository svn://
<SUBVERSION_MACHINE>:3690/svn_repository \\<SUBVERSION_SHARE>\CheckOut
\<WORKSPACE_NAME>-LCMB6400\WORKSPACE
```

5. When prompted enter the password of the operating system administrator, the user, and the password.

> **Note**
>
> By default, the user is LCM and the poassword that had been set during installation.

6. In the CMC, on the Version Management System settings page, change the *Server Name* from **localhost** to the address of your main machine.
7. Change the *Workspace Directory* from **localhost** to your working copy share: **<SUBVERSION_SHARE>**\CheckOut
8. Stop the Server Intelligence Agent (SIA) and change the account from LocalSystem to the operating system administrator

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9. Start the SIA.

> **Note**
>
> If the SIA has already been running under an account with network access to the shared directory, you only need to restart all the Processing Job Servers that host the VMS..

16.7.3 Configuring other Subversion machines

To configure other Subversion machines, stop the Server Intelligence Agent (SIA) and change the account from LocalSystem to an account that has network access, so that this Processing Job Server can access the shared directory (for example, the operating system administrator account). Then, restart the SIA.

> **Note**
>
> If the SIA has already been running under an account with network access to the shared directory, you only need to restart all the Processing Job Servers that host the VMS..

16.8 To access the same ClearCase view from multiple Version Management Servers

1. Set up the main ClearCase machine.

   This machine will host the internal files and metadata that ClearCase uses. Otherr machines will connect to this machine.
2. Set up a slave ClearCase machine.

   This machine will connect and share the views of the main ClearCase machine.

   > **Remember**
   >
   > Do note install any server components (such as the Versioned Object Base (VOB) Server or the View Server) with the ClearCase packages
3. Add the name of the main ClearCase machine to use it as the registry server.
4. Do not follow the steps in the “Create VOB” section. Start the main view locally and mount the VOB.
   a. Establish the name of the workspace using one of the following methods:
      - Perform a Version Management System (VMS) operation using the main machine. Then, inspect the Subversion working copy directory to determine the name of the workspace.
      - Calculate the name of the workspace by removing the symbol @ and replacing all colons with the character *B*. For example, if the cluster is named `ABCD-LCM:6400`, the VMS will use `ABCD-LCMB6400` as the workspace name.

   b. Bring up the view locally by running the following command: **`cleartool startview <VIEW_NAME>`**
   The view will appear on the slave ClearCase machine.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

c. Mount the VOB by running the following command: **`cleartool mount \<VOB_TAG>`**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

17 Visual Difference

17.1 Visual Difference in the promotion management tool

Visual Difference allows you to view the differences between two versions of a supported file type (LCMBIAR) or a supported object type (LCM Job) or both. You can use this feature to determine the difference between files or objects to develop and maintain different report types. This feature gives a comparison status between the source and the destination versions. For example, if a previous version of the user report is accurate and the current version is inaccurate, you can compare and analyze the file to evaluate the issue.

> **Note**
>
> To use Visual Difference, you must install Adobe Flash Viewer.

The following are the three types of visual difference from which you can detect the file or an object:

- Removed - In a report, if an element is missing in one of the file versions, the type of difference is shown as Removed. For example, the element could be a row, section instance, or even a block.
- Modified - In a report, if there is a different value between the source version and the destination version, the type of difference is shown as Modified. For example, the value could be the cell content or the result of a local variable.
- Inserted - In a report, if there is an element in the destination version but is not present in the source version, the type of difference is shown as Inserted.

The following are the object types that support visual difference:

- LCMBIAR
- Promotion Management Job

You can compare the following combinations:

- A Promotion Management job with another Promotion Management job
- A Promotion Management job with an LCMBIAR file
- An LCMBIAR file with another LCMBIAR file
- An LCMBIAR file with a Promotion Management job

Preferences

On the visual difference home page, you can set preferences such as product locale, preferred viewing locale, maximum number of objects per page, time zone, and prompting for unsaved data.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Home Page

The visual difference home page consists of the following tabs and panes:

- New Comparison - this tab allows you to create new comparison between objects
- Search Comparisons - this field allows you to search for the already compared objects
- Comparisons pane - this pane lists the filters and differences tabs
- Comparisons: Differences pane - this pane lists the compared objects with the comparison name, Date/Time and the status of the differences

17.1.1 To compare objects or files using Visual Difference

The visual difference option allows you to compare the BIAR files and objects.

To compare files using visual difference, complete the following steps:

1. Log into the CMC application.
2. In the CMC homepage, under the *Manage* tab, click the *Visual Difference* link.
   The Visual Difference page is displayed. The compared files are stored in the "Differences" folder, or in any of the user created sub-folders.

   > **Note**
   >
   > To create a new sub-folder, click the Folder icon.

3. Click *New Comparison*.
   The *Visual Difference - Comparisons* screen is displayed.
4. Select the reference system from the *Select System* under Reference.

   You can connect to any of the following reference systems:

   - CMS
   - VMS
   - Local File System
5. Click *Browse* to select the object, or a file from your local system that you want to compare.
6. Select the target system from the *Select System* under Target.

   You can connect to any of the following reference systems:

   - CMS
   - VMS
   - Local File System

   > **Note**
   >
   > If you log into the CMS or the VMS, the selected object in the reference system can also be automatically matched with an object having the same name in the reference system.

7. Click *Browse* to select the object or a job from your local system that you want to compare.
8. Click *Add*.
   The objects selected for comparison are added to the shopping cart.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

If more than one of pair of objects is added to the shopping cart, the objects can be scheduled for comparison at a later time. However, if the shopping cart contains just one pair of objects, you can compare these objects.

To compare the files, continue with the next step. To schedule the comparison, see To schedule the comparison [page 540].

9. Click *Compare* to compare the objects or folders.

> **Note**
>
> The comparison of LCMBIAR/Promotion Management Job file includes:
>
> - LCMBIAR Metadata: comparison of the job details like name, created by, time.
> - Primary Objects: comparison of each of the explicitly selected objects in the LCMBIAR against a similar object in the target LCMBIAR by CUID.
> - Dependent Objects: comparison of the selected dependent object in the file against a similar object in the target by CUID.
>
> If the objects other than LCMBIAR or Promotion Management job are selected, the following error message is displayed: `Plugin not found.`

The comparison process starts immediately and the differences if any are displayed in the *Visual Difference viewer*. The differences are highlighted in orange color, and the missing objects are highlighted in red color.

You can also use the filter option to view the compared objects by type, and with differences or with common attributes.

10. Click *Save* to save the difference report.
11. Specify the location where you want to save the report, and click *OK*.

17.1.2 To compare objects or files using the Version Management System

You can compare promotion management jobs or folders in a version management system using the visual difference option.

To compare objects in a version management system, complete the following steps:

1. Log on to the CMC application.
2. In the CMC homepage, under the *Manage* tab, click the *Visual Difference* link.
   The Visual Difference page is displayed. The compared files are stored in the "Differences" folder, or in any of the user created sub-folders.

> **Note**
>
> To create a new sub-folder, click the Folder icon.

3. Click *New Comparison*.
   The *Visual Difference - Comparisons* screen is displayed.
4. Select *Logon to VMS* from *Select System* under Reference.
5. Enter the login credentials to the VMS, and click *Log On*.
   The *Visual Difference - Auto Select Target System* dialog box is displayed

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Click *No* if you want to set a different target system, or click *Yes* if you want to set the target system same as the reference system.
7. Click *Browse* to select the objects or jobs that you want to compare from both the reference and target systems.
8. Click *Add*.
   The objects selected for comparison are listed in the *New Comparison* pane.
   You can compare the files immediately, or schedule the comparison for a later point of time. To compare the files, continue with the next step. To schedule the comparison, see To schedule the comparison [page 540].
9. Click *Compare* to compare jobs or folders.
   The comparison process starts immediately and the differences if any are displayed in the *Visual Difference viewer*. The differences are highlighted in orange color, and the missing objects are highlighted in red color. You can also use the filter option to view the compared objects by type, and with differences or with common attributes.
10. Click *Save* to save the difference report.
11. Specify the location where you want to save the report, and click *OK*.

17.1.3 To schedule the comparison

To schedule the comparison of files or objects, complete the following steps:

1. Click *Schedule*.
   The *Visual Difference -Schedule* window is displayed.
2. Select the frequency to schedule the comparison from the *Run Comparison* list.
3. Specify the number of retries allowed, and the retry interval in the respective fields.

   > **Note**
   >
   > You can specify the retry interval only if you specify the number of retries.

4. Specify the report name, and click *Browse* to browse for the location in which you want to save the report.
   The *Save Job in* window is displayed.
5. Select the required folder where you want to save the report, and click *OK*.

   > **Note**
   >
   > Depending on the option you select from the *Run Comparison* list, you must specify the date and time respectively for comparison.

6. Click *Schedule*.

   The user can view the comparison object or the difference report in the Visual Difference Viewer at a later point of time. The *Compared Differences* page is displayed with the list of folders and files or comparison reports.

   The Compared Difference page also contains the following options:

   - *History* This option allows you to view the history of comparison.
   - *Rerun* This option runs the comparison again.
   - *Schedule* This option allows you to schedule the comparison.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18 Managing Applications

18.1 Managing applications through the CMC

18.1.1 Overview

The *Applications* management area of the CMC allows you to change the appearance and functionality of web applications such as the CMC and BI launch pad, without doing any programming. You can also modify access to applications for users, groups, and administrators by changing the rights associated with each one.

In this section, you'll find contextual information, procedures, and instructions on how to manage various settings. The following applications have settings that can be modified through the CMC:

- Alerting Application
- Analysis edition for OLAP
- BEx Web Applications
- BI launch pad
- BI workspaces
- Central Management Console
- Collaboration (with SAP Jam or SAP StreamWork)
- Crystal Reports Configuration
- Dashboards
- Desktop Intelligence
- Discussions
- HANA Authentication
- Information Design Tool
- Monitoring application
- Multitenancy Management Tool
- Information Steward Application
- Open Document
- Platform Search Application
- Promotion Management
- Report Conversion Tool
- SAP BusinessObjects Mobile
- SAP Lumira
- Translation management tool
- Universe design tool
- Upgrade management tool
- Version Management
- Visual Difference
- Web Intelligence
- RESTful Web Service

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Web Service
- Widgets

18.1.2 Common settings for applications

18.1.2.1 Setting user rights on applications

You can use rights to control user access to certain features of applications. The *Applications* area in the CMC lets you assign principals to the access control list for an application, view the rights that a principal has, and modify the rights that the principal has to an application. For more information about rights administration, see the *SAP BI platform Administrator Guide*.

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

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

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

   > **Note**
   >
   > These applications have trace log settings: BI launch pad, CMC, Open Document, Promotion Management, Version Management, Visual Difference, and Web Service.

   The *Trace Log Settings* dialog box appears.
2. Select a setting from the *Log Level* list.
3. Click *Save & Close*.

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

Related Information

Trace log levels [page 542]

18.1.2.2.1 Trace log levels

The following trace log levels are available for BI platform components:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Level	Description
Unspecified	The trace log level is specified through other means (usually an `.ini` file).
None	No tracing occurs.
Low	The trace log filter allows logging error messages while ignoring warning and status messages. Important status messages are logged for component startup, shutdown, start request, and end request messages. This level is not recommended for debugging purposes.
Medium	The trace log filter is set to include error, warning, and most status messages. Least important or highly verbose status messages are filtered out. This level is not verbose enough for debugging purposes.
High	No messages are filtered. This level is recommended for debugging purposes. **⚠ Caution** This trace log level significantly affects system resources, increasing CPU usage and consuming storage space.

18.1.3 Application-specific settings

18.1.3.1 Managing CMC application settings

18.1.3.1.1 Authentication and program objects

You can control the types of program objects users can run, and you can configure the credentials required to run program objects.

Be aware of the potential security risks associated with adding program objects to the repository. The level of file permissions for the account under which a program object runs will determine what modifications, if any, the program can make to files.

Enabling or disabling a type of program object

As a first level of security, you can configure the types of program objects available for use.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authentication on all platforms

In the *Folders* management area of the CMC, you must specify credentials for the account under which the program runs. This feature allows you to set up a specific user account for the program, and assign it appropriate rights, to have the program object run under that account.

Alternatively, users who add program objects to nformation platform services can assign their own credentials to a program object and give the program access to the system. Thus, the program will run under that user account, and the rights of the program will be limited to those of the user. If you choose not to specify a user account for a program object, it runs under the default system account, which generally has rights locally but not across the network.

> **Note**
>
> By default, when you schedule a program object, the job fails if credentials are not specified. To provide default credentials, select *CMC* in the *Applications* management area. On the *Actions* menu, click *Program Object Rights*. Click *Schedule with the following operating system credentials* and provide a default user name and password.

Authentication for Java programs

Information platform services allows you to set security for all program objects. For Java programs, Information platform services forces the use of a Java Policy File, which has a default setting that is consistent with the Java default for unsecured code. Use the Java Policy Tool (available with the Java Development Kit) to modify the Java Policy File, to suit your specific needs.

The Java Policy Tool has two code base entries. The first entry points to the SAP BusinessObjects Enterprise Java SDK and allows program objects full rights to all SAP BusinessObjects Enterprise JAR files. The second code base entry applies to all local files. It uses the same security settings for unsecured code as the Java default for unsecured code.

> **Note**
>
> The settings for the Java Policy are universal for all Program Job Servers running on the same machine.

> **Note**
>
> By default, the Java Policy File is installed to the Java SDK directory in the Information platform services install root directory. For example, a typical location on Windows is: `C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

18.1.3.1.1.1 To enable or disable a type of program object

1. In the *Applications* area, select *Central Management Console*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Click *Actions* > *Program Object Rights*.
   The *Program Object Rights* dialog box appears.
3. In the *Allow users to* area, select the types of program objects that you want users to be able to run.

   You can select *Run scripts/binaries* or *Run java programs*.

   If you selected *Run java programs*, you can select or clear the *Use impersonation* check box. This option provides the Java program a token with which to log on to Information platform services.
4. Click *Save & Close*.

18.1.3.1.2 Registering processing extensions with the system

> **Note**
>
> This feature does not apply to Web Intelligence documents.

Before you can apply your processing extensions to particular objects, you must make your library of code available to each machine that will process the relevant schedule or view requests. Installing the BI platform creates a default directory for your processing extensions on each Job Server, Processing Server, and Report Application Server (RAS). It is recommended that you copy your processing extensions to the default directory on each server. On Windows, the default directory is `C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ProcessExt`. On UNIX, it is the `sap_bobj/ProcessExt` directory.

> **Tip**
>
> It is possible to share a processing extension file.

Depending upon the functionality that you have written into the extension, copy the library onto the following machines:

- If your processing extension intercepts schedule requests only, copy your library onto each machine that is running as an Adaptive Job Server.
- If your processing extension intercepts view requests only, copy your library onto each machine that is running as a Crystal Reports Processing Server or RAS.
- If your processing extension intercepts schedule and view requests, copy your library onto each machine that is running as an Adaptive Job Server, Crystal Reports Processing Server, or RAS.

> **Note**
>
> If the processing extension is required only for schedule/view requests made to a particular server group, you need only copy the library onto each processing server in the group.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.1.2.1 To register a processing extension with the system

1. Go to the *Applications* management area of CMC.
2. Select *Central Management Console*.
3. Click *Actions* > *Processing Extensions*.
   The *Processing Extensions: CMC* dialog box appears.
4. In the *Name* field, enter a display name for your processing extension.
5. In the *Location* field, type the file name of your processing extension along with any additional path information.
   - If you copied your processing extension into the default directory on each of the appropriate machines, just type the file name (but not the file extension).
   - If you copied your processing extension to a subfolder below the default directory, type the location as: **`<subfolder>/<filename>`**
6. Use the *Description* field to add information about your processing extension.
7. Click *Add*.

> **Tip**
>
> To delete a processing extension, select it from the *Existing Extensions* list and click *Delete*. (Make sure that no recurring jobs are based on this processing extension because any future jobs based on this processing extension will fail.)

8. Click *Save & Close*.
   The processing extension is registered with CMC.

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

18.1.3.1.2.2 Sharing processing extensions between multiple servers

> **Note**
>
> This feature does not apply to Web Intelligence documents or reports created in SAP Crystal Reports for Enterprise.

If you want to put all processing extensions in a single location, you can override the default processing extensions directory for each Adaptive Job Server, Crystal Reports Processing Server, and RAS. First, copy your processing extensions to a shared directory on a network drive that is accessible to all of the servers. Map (or mount) the network drive from each server's machine.

> **Note**
>
> Mapped drives on Windows are valid only until you reboot the machine.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

If you are running servers on both Windows and on UNIX, you must copy a .dll and an .so version of every processing extension into the shared directory. In addition, the shared network drive must be visible to Windows and to UNIX machines (through Samba or some other file-sharing system).

Finally, change each server's command line to modify the default processing extensions directory. To change the command line, go to the Servers tab in the CMC, select a server, and open its Properties page. Add `-report_ProcessExtPath <absolute path>` to the command line. Replace **<absolute path>** with the path to the new folder, using whichever path convention is appropriate for the operating system that the server is running on (for example, `M:\code\extensions`, `/home/shared/code/extensions`, and so on).

To modify the default processing extensions directory, use the CMC to stop the server. Then open the server's Properties to modify the command line. Start the server again when you have finished.

18.1.3.1.3 Managing CMC tab access

18.1.3.1.3.1 Delegated administration and CMC tab access

Typically, a BI platform system administrator manages a large number of documents, folders, users, servers, and other objects. However, large corporate environments may exceed the resources of a single administrator. A system administrator who wants to focus only on high-priority tasks can create delegated administrators and assign subsets of management tasks to them (for example, the administration of a department or tenant content). Unlike system administrators, delegated administrators perform a limited set of tasks and have fewer rights on objects in the system.

The default configuration of the Central Management Console allows users to access all available CMC tabs. The system administrator can manage CMC tab access to control which tabs are visible to principals (users or user groups). To improve the user experience and workflow of the delegated administrator, a system administrator may also hide any of the CMC tabs that a delegated administrator is not expected to use.

> ⚠ Caution
>
> Management of CMC tab access affects only the visual appearance of the CMC user interface. Hiding CMC tabs is not a security measure, because it does not set or modify security rights on objects within tabs. To ensure that users cannot perform unauthorized operations on unauthorized objects (for example, manage servers through the Central Configuration Manager or third-party software based on the BI platform SDK), you must set appropriate security rights on objects (such as server objects).

Related Information

To manage CMC tab access for other users [page 549]
To manage permission to configure CMC tab access for other users or user groups [page 551]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.1.3.2 Working with CMC tab access

18.1.3.1.3.2.1 Managing CMC tab access for other users

A system administrator always has access to all CMC tabs. Use the following guidelines to administer the CMC tabs that principals can access:

- For a simplified management process and a reduced need for maintenance and troubleshooting, it is recommended that administrators manage CMC tab access on a user group level (instead of on a user level).
- For CMC tabs that have top-level folders, an administrator must grant access to a tab and grant the *View* right on the top-level folder of the tab. The following CMC tabs support top-level folders:
  - *Access Levels*
  - *Calendars*
  - *Categories*
  - *(Universe) Connections*
  - *Cryptographic Keys*
  - *Events*
  - *Federations*
  - *Folders*
  - *Inboxes*
  - *OLAP Connection*
  - *Personal Categories*
  - *Personal Folders*
  - *Profiles*
  - *Replication Lists*
  - *Servers and Groups*
  - *Temporary Storage*
  - *Universes*
  - *Users and Groups*
  - *Web Service Query*
- For improved system security, only members of the Administrators group can access the following CMC tabs. As system administrators, members of the Administrators group can access any CMC tab regardless of CMC tab access permissions. CMC tab access permissions are designed to control access to CMC tabs for delegated administrators; that is, users other than members of the Administrators group.
  - *Auditing*
  - *Authentications*
  - *Cryptographic Keys*
  - *License Keys*
  - *Monitoring*
  - *Sessions*
  - *Settings*
  - *User Attribute Management*

Caution

Management of CMC tab access affects only the visual appearance of the CMC user interface. Hiding CMC tabs is not a security measure, because it does not set or modify security rights on objects within tabs. To ensure

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

that users cannot perform unauthorized operations on unauthorized objects (for example, manage servers through the Central Configuration Manager or third-party software based on the BI platform SDK), you must set appropriate security rights on objects (such as server objects).

18.1.3.1.3.2.1.1 To manage CMC tab access for other users

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

   > **Note**
   >
   > If CMC tab access is unrestricted, the following message will be displayed: `Warning: CMC tab access is currently unrestricted. To restrict CMC access, click the "Application" tab, select "CMC," and set the CMC tab access to restricted. These settings take effect after CMC tab access is restricted.` You can still configure CMC tab access. However, the configuration will not take effect until you restrict CMC tab access.

   In the *Configure CMC Tab Access* dialog box, a table is displayed:

   - ✓ or ✗ indicates which CMC tabs the principal can access.
   - *Inherited* indicates that the tab access was inherited from its parent user group(s).
   - *Explicit* indicates that the tab access was explicitly specified on the principal level.
3. Review the CMC tab access rights. To modify the rights, you can use the buttons on the toolbar:
   - Click *Grant* to explicitly grant access to a tab.
   - Click *Deny* to explicitly deny access to a tab.
   - Click *Inherit* to use an inherited access right.

   > **Note**
   >
   > Clicking the buttons applies changes to the principal immediately.
4. When you are finished, click *Close*.

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

Related Information

To restrict CMC tab access [page 552]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.1.3.2.1.2 Inheritance of CMC tab access

CMC tab access rights and the permission to configure CMC tab access for other users or user groups are both applied and inherited in the same way as other BI platform security rights. If principals have no tab access explicitly specified, they will inherit the tab access of the user groups they are members of.

If a user is a member of two user groups, tab access is calculated in the same manner as all other BI platform rights are calculated. For example, if access to a CMC tab is granted in one of the groups and denied in the other, the principal will not be able to access the CMC tab.

> **Note**
>
> - Modifying the CMC tab access right of a user group changes the same tab access for all users or user groups that inherit rights from the user group, if their CMC tab access is set to *Inherited*.
> - Tab access set on the user level always supersedes tab access inherited from user groups.

18.1.3.1.3.2.1.3 Delegated administrator user groups

You can create a set of delegated administrator user groups to simplify CMC tab management. To avoid configuring individual CMC tab access, you can make an existing user or user group a member of a delegated administrator user group. The following configuration is recommended, but it can be modified for specific business needs.

> **Note**
>
> Membership in multiple groups will result in the addition of rights, if the rights are set to *Inherited*.

Delegated Administrator User Group	Recommended Rights
System Administrators	Grant access to all tabs.
User Administrators	Grant access to *Access Levels*, *Folders*, *Inboxes*, *Personal Folders*, *Personal Categories*, *Query Results*, *Sessions*, and *User and Groups*. Set all other tabs to *Inherited*.
Content Administrators	Grant access to *Calendars*, *Categories*, *Events*, *Folders*, *Instance Manager*, *Personal Categories*, *Personal Folders*, *Profiles*, *Query Results*, and *Universes*. Set all other tabs to *Inherited*.
Server Administrators	Grant access to *Servers* and *Applications.* Set all other tabs to *Inherited*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

In a large corporate environment, a system administrator may need to delegate CMC tab access management to a delegated administrator. Alternatively, in a multitenant system each tenant may have a delegated administrator responsible for managing CMC tab access for other users and user groups.

1. Log onto the CMC.
2. On the *Users and Groups* tab, right-click a principal and select *CMC Tab Configuration*.
   In the *Configure CMC Tab Access* dialog box, the *Permission to configure CMC tab access for other users or user groups* is displayed for the principal.

   > **Note**
   >
   > If this permission is granted, the principal will be able to manage CMC tab access (only for tabs that the principal has access to) for users on which the principal has the *Securely Modify Rights* right. In addition, the principal will be able to further delegate CMC tab access management to other users by granting the *Permission to configure CMC tab access for other users or user groups* to users on which the principal has the *Securely Modify Rights* right.

   - ✓ or ✗ indicates whether the principal has permission to configure CMC tabs for other users or user groups.
   - *Inherited* indicates that the permission was inherited from its parent user group(s).
   - *Explicit* indicates that the permission was explicitly specified on the principal level.
3. Review the permissions to configure CMC tab access for other users or user groups. To modify the permissions, you can select one of the following settings from the list:
   - Click *Grant* to explicitly grant permission to manage CMC tab access for other users or user groups.
   - Click *Deny* to explicitly deny permission to manage CMC tab access for other users or user groups.
   - Click *Inherit* to inherit permission to managed CMC tab access for other users or groups.

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

The new effective permission is displayed.

Related Information

Delegated administration and CMC tab access [page 547]
Inheritance of CMC tab access [page 550]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

1. In the CMC, go the *Users and Groups* management area.
2. Right-click a user or user group and select *CMC Tab Configuration*.

   The *Configure CMC Tabs* dialog box appears, listing each CMC tab title and its permission level, for the user group.

   If the following warning message appears in red at the top of the dialog box, you must set CMC tab access to restricted before you can add a *Customization* tab:

   ```
   Warning: CMC tab access is currently unrestricted. To restrict CMC access, click
   the "Application" tab, select "CMC," and set the CMC tab access to restricted.
   These settings take effect after CMC tab access is restricted:
   ```
3. (If necessary) To set CMC tab access to restricted:
   a. In the *Applications* management area of the CMC, right-click *Central Management Console* and select *CMC Tab Access Configuration*.
   b. Under *CMC Tab Access*, select the *Restricted* option, and click *Save & Close*.
4. In the *Configure CMC Tabs* dialog box for the user group, for each CMC tab, select *Granted*, *Denied*, or *Inherited* in the list.
   Each time you change the permission for a tab, the Configure CMC Tabs dialog box updates the user group's permission to configure tab access for other users or user groups.
5. Click *Close*.

18.1.3.1.3.2.2 To restrict CMC tab access

It is recommended that you first configure CMC tab access for principals, and then restrict CMC tab access. If you restrict tab access before configuring it, your users will not be able to access any CMC tabs until an administrator grants them access.

To ensure consistency with previous versions of the BI platform, CMC tab access is initially unrestricted after the BI platform is installed, and any user who can access the CMC is able to access all available tabs. To prevent users from accessing tabs to which they have no access rights, a system administrator can restrict CMC tab access.

You can remove CMC tab access restriction in an urgent case, or to troubleshoot CMC tab access configuration (for example, if a delegated administrator cannot access an essential CMC tab).

1. Log onto the CMC.
2. On the *Applications* tab, right-click *Central Management Console* and select *CMC Tab Access Configuration*.
   The *CMC Tab Access* dialog box is displayed.
3. Configure the CMC tab access rule.
   - To limit your users to access to tabs for which they have rights, select *Restricted*.
   - To allow your users to access all tabs, select *Unrestricted*.
4. When you are finished, click *Save and Close*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The CMC tab access rule is applied to the system.

Related Information

To troubleshoot CMC tab access [page 553]

18.1.3.1.3.2.3 To troubleshoot CMC tab access

To prevent unauthorized access, or to troubleshoot a user's limited access to CMC tabs, you can troubleshoot a user's CMC tab access rights.

1. Log onto the CMC as an administrator.

   > **Note**
   >
   > Ensure you have access to the tab that you want to troubleshoot, and that you have the *Securely Modify Rights* right on the user.

2. On the *Users and Groups* tab, right-click a principal and select *CMC Tab Configuration*.
   The *Configure CMC Tab Access* window is displayed.
3. Review the effective CMC tab access. You can explicitly grant or deny access to available tabs.
   If the CMC tab access is inherited, but the effective tab access does not match the user's needs:
   a. Compile a list of all user groups that the selected principal is a member of.
   b. Repeat steps 1-3 for every group that the user inherits tab access from.
   c. Correct CMC tab access on the principal level or under the group level as needed.

   > **Note**
   >
   > Performing this task on the group level affects CMC tab access for all users who are members of this user group, and all users who are members of user groups inherited from this user group, as long as the users have CMC tab access set to *Inherited*.

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

Related Information

To manage CMC tab access for other users [page 549]
Inheritance of CMC tab access [page 550]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.2 Managing discussion settings

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

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

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

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

18.1.3.2.1 To search for a discussion thread

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

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

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

Option	Description
Thread title	Searches by thread title.
Creation date	Searches by creation date.
Last modified date	Searches by the last date modified.
Author	Searches by author.

4. On the second list, refine your search.

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

18.1.3.2.2 To sort your discussion thread search results

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

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

Option	Description
Thread title	Sort by the title of a discussion thread.
Creation date	Sort by the date the discussion thread was created.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

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

18.1.3.2.3 To delete a discussion thread

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

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

18.1.3.3 Managing BI launch pad settings

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

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

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

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

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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.3.1 To change display settings for BI launch pad

1. Go to the *Applications* area of the CMC, and double-click *BI launch pad*.
   The *BI Launch Pad Properties* dialog box appears.
2. To enable discussions for BI launch pad users, select the *Enable Discussions* check box.
3. To enable filters for scheduling, select the *Show the "Filters" tab on the Schedule page* check box.
   This setting controls whether users can enter record or group selection formulas when scheduling a Crystal report.
4. Click *Save & Close*.

18.1.3.4 Managing Web Intelligence settings

You can control which features your users have access to for Web Intelligence documents by setting properties for the Web Intelligence application.

18.1.3.4.1 To modify display settings for Web Intelligence

1. Go to the *Applications* area of the CMC and select *Web Intelligence*.
2. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
3. Define any of the following display options.

Option	Description
Dimensions and details	Use the options in this area to define how added data appears in reports; change the font style, text color, and background color. A cell preview automatically shows your changes. Click *OK* when you are finished.
Fluctuating values (numerical measures)	Use the options in this area to modify and format the page heading; change the font style, text color, and background color. A cell preview automatically shows your changes. Click *OK* when you are finished.
Embedded image properties	Enter the maximum embedded image size.
Quick display mode properties	In the appropriate fields, enter the maximum vertical records, maximum horizontal records, minimum width of page, minimum height of page, right padding value, and bottom padding value.
Auto-save Settings	Set the interval at which documents are autosaved. This interval is reset each time a document is saved manually or automatically. The autosaved document is also deleted when you save a document manually.
Automatic Refresh	Enables automatic refreshing of Web Intelligence documents when the Web Intelligence document property *Auto-refresh* is selected. For details, see the *SAP BusinessObjects Web Intelligence User Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Auto-Merge	Enables automatic merging of dimensions when the Web Intelligence document property *Auto-merge dimensions* is selected. For details, see the *SAP BusinessObjects Web Intelligence User Guide*.
Automatic Document Refresh on Open Security Right Setting	Clear this option to enable Web Intelligence to refresh documents automatically on opening, without enabling *Refresh on open* in the Web Intelligence document properties. Selecting this option selects the security right *Documents - disable automatic refresh on open*.
Smart View	This option determines which document version is displayed when users open documents in Web Intelligence. ○ View Latest Instance The latest instance of the object is opened. For example, if a document is scheduled for a refresh every hour, and the document was last saved and closed five hours ago, the latest instance is opened. When a user saves that instance, the original document is updated accordingly. ○ View Object The document is opened in the same state as when it was last saved, irrespective of any scheduled refreshes that might have occurred.

4. Click *Save & Close*.

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

18.1.3.5 Managing alerting settings

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

For the *Alerting* application you can control and define how system users access alerts by:

- Enabling the *My Alerts* folder for alert subscribers
- Enabling and formatting alert messages sent through email
- Setting a limit for the number of alerts in the system
- Setting an expiry period for alert messages

Related Information

Setting user rights on applications [page 542]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.5.1 To modify alerting destination properties

1. In the *Applications* area of the CMC, double-click *Alerting Application*.
2. Click *Manage* > *Properties*.
   The *Alerting* dialog box appears.
3. (Required) Perform one of the following actions:
   - Select *Enable My Alerts* to enable alert subscribers to receive notifications under *My Alerts* in BI launch pad.
   - Select *Enable Email* to enable alert subscribers to receive notifications through email.
     Global email options for alerts appear.
4. If you selected *Enable Email*, perform the following actions:
   - In the *From* box, enter the email address that alert notifications will be sent from.
     Subscribers will receive alert emails from this email address. Use a valid email address that is recognized by your system.
   - In the *To* box, enter the email address of the alert subscriber.
     By default, all system alerts will be sent to this email address.

     > **Tip**
     >
     > Do not specify a email address or recipient. Use the *%SI_EMAIL_ADDRESS%* placeholder.

   - In the *cc* box, enter each recipient email address that should receive carbon copies of alerts.
   - In the *Subject* box, enter a default subject heading to use in emails containing alerts.
   - In the *Message* box, enter a default message to include in emails containing alerts.
   - Select *Add Attachment* to enable attachments to be included by default in emails containing alerts.
     For example, select this option to include associated Crystal reports with triggered alerts.
   - If you selected *Add Attachment*, in the *File Name* select *Automatically Generated* or *Specific Name* to indicate how to name attachments in emails.
5. Click *Save & Close*.

Related Information

Setting user rights on applications [page 542]
Managing alerting settings [page 558]

18.1.3.5.2 To modify Alerting default properties

1. Go to the *Applications* area of the CMC and select *Alerting Application*.
2. Click *Manage* > *Properties* > *Default Settings*.
3. Set the appropriate values for the following properties.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Expiry Period	Specifies how long alert messages will be maintained in the system before they are deleted.
Maximum Number of Alert Messages	Specifies the maximum number of alert messages supported by the system. When the threshold is reached, the system will remove 20% of the alert messages, starting with the oldest messages.

4. Click *Save & Close*.

Related Information

Managing alerting settings [page 558]

18.1.3.6 Managing widgets settings

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

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

You can grant users or groups the ability to:

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

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

18.1.3.7 Managing SAP BusinessObjects Explorer settings

You can define which features your users have access to for SAP BusinessObjects Explorer by settings its security rights from the Applications area of the CMC.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.7.1 To modify SAP BusinessObjects Explorer application properties

1. Go to the *Applications* area of the CMC.
2. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
3. Define any of the following SAP BusinessObjects Explorer settings:
   - Bookmark Validity
   - Advanced Configuration
4. Click *Save & Close*.

18.1.3.8 Managing collaboration-application integration

This guide is intended for BI platform administrators who will integrate the BI platform with a SAP Jam or SAP StreamWork collaboration application.

Use the *Applications* area of the Central Management Console (CMC) in the BI platform to enable and configure collaboration.

The following additional configuration is required in the collaboration application's Enterprise Agent:

- Establish an HTTPS connection with a service provider
- Fulfill prerequisites for authentication

After SAP Jam or SAP StreamWork is configured, feeds from the collaboration application are available in the BI launch pad.

SAP Jam does not support Microsoft Internet Explorer 11.

18.1.3.8.1 Collaboration prerequisites

Collaboration prerequisites must be met before you integrate the BI platform with a collaboration application.

- The BI platform must be installed with at least one Central Management Server (CMS).
- The collaboration application (SAP Jam or SAP StreamWork) must be configured in the Central Management Console (CMC).
- A collaboration application (SAP Jam or SAP StreamWork) Enterprise organization must be defined.
- SAP Jam or SAP StreamWork users must belong to the Enterprise organization.
- An SAP Jam or SAP StreamWork Enterprise Agent is required to provision users who use an on-premise LDAP/AD directory service.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.8.2 BI platform configuration

18.1.3.8.2.1 Collaboration configuration options

Collaboration options appear in the *Properties: Collaboration* dialog box in the Central Management Console (CMC) in the BI platform.

To access the *Properties: Collaboration* dialog box, on the *Applications* tab in the CMC, click *Collaboration*, and select *Manage* > *Properties*.

Table 82:

Option	Description	
Enable Collaboration	Select this check box, and select *SAP Jam* or *SAP StreamWork*.	
Connection URL	Enter the URL to the collaboration application.	
Unique Identity Provider ID	Enter a unique value for your BI platform deployment. The value should be associated with the certificate used to configure integration on the collaboration application's administration console. The application asserting an identity for single sign-on must be configured as an administrative OAuth application.	
Identity Provider Base64 Certificate	When you click *Generate*, a certificate is created in this box. Use the certificate in the collaboration application's administration console to generate an OAuth Consumer Key. The certificate establishes the trust relationship between the collaboration application and the BI platform. The external identity provider itself is identified with an X509 certificate, which is used to sign all identity assertions. The certificate must be Base64-encoded.	
OAuth Consumer Key	Enter the OAuth Consumer Key that was generated from the collaboration application's administration console.	
Connecting using proxy	Select this check box to enable connection through proxy, and enter information about the proxy host in the *HTTP Proxy Host* and *Port* boxes. To allow inbound connections from collaboration application servers to your corporate network, you must have a reverse proxy in the DMZ. To add a trusted certificate from an SSL certificate provider to the reverse proxy, you must have a domain or subdomain name for the reverse proxy.	
	HTTP Proxy Host	In the reverse proxy configuration, enter an external address that is accessible to the collaboration application. For example, use `https://<ReverseProxy>/`, where `<ReverseProxy>` is the domain or subdomain name of the reverse proxy. The collaboration application uses this address to send information to the BI platform. The reverse proxy uses this address to redirect information received from the collaboration application to the machine containing the collaboration application's Enterprise Agent.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description	
	Port	The collaboration application's Enterprise Agent is configured to listen from port 8443.

18.1.3.8.2.2 Enabling and configuring collaboration in the CMC

This task requires a valid connection to the collaboration application's (SAP Jam or SAP StreamWork) administration console. You will need to pass and retrieve security details from the console.

For security reasons, the following default accounts cannot send or schedule content to SAP Jam or SAP StreamWork:

- Guest
- SMAdmin
- Administrator
- WaaWSServletPrincipal

1. In the Central Management Console (CMC) in the BI platform, go to the *Applications* area, and double-click *Collaboration*.
2. In the *Properties: Collaboration* dialog box, select the *Enable Collaboration* check box, and select *SAP Jam* or *SAP StreamWork*.
3. In the *Connection URL* box, enter the URL to the collaboration application.
4. In the *Unique Identity Provider ID* box, enter a unique identity provider value for your BI platform deployment.

   Make a note of the identity provider value; you will use it to configure the collaboration application.
5. Click *Generate* (or *Regenerate*, if a certificate has been created before).
   The certificate appears in the *Identity Provider Base64 Certificate* box. You will use the certificate to configure the collaboration application.
6. In the *OAuth Consumer Key* box, enter a valid OAuth Consumer Key.
7. If you are connecting via proxy to the server running SAP Jam or SAP StreamWork, perform the following actions:
   a. Select the *Connecting using proxy* check box.
   b. In the *HTTP Proxy Host* box, enter the proxy host name of the server.
   c. In the *Port* box, enter the port number of the server.
8. Click *Save & Close*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.8.3 SAP Jam configuration

18.1.3.8.3.1 Registering a new SAML trusted IDP for SAP

You must register each user with a unique email address that corresponds to the user's Enterprise email address in the BI launch pad. The email addresses will be mapped between the BI platform and SAP.

Before you can register a new SAML trusted IDP:

- Your company must be added to and configured in SAP.
- You must have a valid SAP user account that is associated with your company in SAP.
- You must have company administration rights for your company in SAP and full administrator rights to the BI platform and the BI launch pad.
- The BI launch pad must be registered as an OAuth client that acts as a representative of the launch pad within SAP.

SAP Jam does not support Microsoft Internet Explorer 11.

1. In the upper-right corner of the Central Management Console (CMC) in the BI platform, select *Administrator* and then select *Admin*.
   Information about your company, including your SAP license, is displayed. Write down or otherwise make note of the information.
2. From the *Admin* menu, select *SAML Trusted ID's*, and click *Register your identity provider*.
   You must register the IDP that you created in the BI launch pad.
3. In the *IDP ID* box, enter the unique identity provider value that was created when SAP was configured in the BI platform.
   If you do not have the value, contact your external application administrator.
   For example, enter **<CompanyName>_<SystemId>_<client>**
4. In the *Single Sign-On URL* box, enter the URL that directly accesses SAP.
   SAP uses this URL for single sign-on with the unique identity provider.
5. In the *Single Log-Out URL* box, enter the URL to display after logging off SAP.
   SAP uses this URL for single log-out with the unique identity provider.
6. In the *Default Name ID Format* box, enter the name ID format to use in authentication requests.
7. In the *Default Name ID Policy SP Name Qualifier* box, enter the SP name qualifier to use in authentication requests.
8. In the *Allowed Assertion Scope* list, select *Users in my company*.
   This option specifies the set of users for which SAP will accept assertions from the IDP.
9. In the *X509 Certificate (Base64)* box, enter the Base64 certificate value that was generated when SAP was configured in the BI platform.
   If you do not have the value, contact your external application administrator.
10. Click *Register*.

18.1.3.8.3.2 Creating an OAuth client for SAP Jam

Before you can create an OAuth Consumer Key:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Your company must be added to and configured in SAP Jam.
- You must have a valid SAP Jam user account that is associated with your company in SAP Jam.
- You must have company administration rights for your company in SAP Jam and full administrator rights in the BI platform and in the BI launch pad.
- The BI launch pad must be registered with SAP Jam as an OAuth client, which acts as a representative of the launch pad within SAP Jam.
- Each user must be registered in SAP Jam with a unique email address that corresponds to the user's Enterprise email address in the BI launch pad. The email addresses will be mapped between the BI platform and SAP Jam.

SAP Jam does not support Microsoft Internet Explorer 11.

1. In SAP Jam, from the *Administrator* menu in the upper-right corner, select *Admin*.
   Information about your company, including your SAP Jam license, appears.
2. From the *Admin* menu, select *OAuth Clients*, and click *Add OAuth Client*.
3. In the *Register a new OAuth Client* dialog box, in the *Name* box, enter the unique identity provider value that was created when SAP Jam was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

   SAP Jam displays the application name as a hyperlink (to the URL you enter) when it takes action on behalf of a user.

   For example, enter **<CompanyName>_<SystemId>_<Client>_<Application>**
4. In the *Integration URL* box, enter the URL for the BI launch pad.

   SAP Jam displays the application name as a hyperlink to the URL when it takes action on behalf of a user.
5. In the *X509 Certificate (Base64)* box, enter the Base64 certificate value that was generated when SAP Jam was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

   If you leave this box blank, SAP Jam supplies a consumer secret.
6. Click *Save*.

The OAuth Consumer Key is generated. Make a note of the OAuth Consumer Key value for the BI platform administrator to use.

18.1.3.8.4 SAP StreamWork configuration

18.1.3.8.4.1 Illustration of SAP StreamWork integration

This diagram shows required BI platform, SAP StreamWork, and SAP StreamWork Enterprise Agent components for integration with SAP StreamWork.

The workflow describes the steps involved in integrating the systems and an overview of the actions users can perform after the integration:

- In the SAP StreamWork Enterprise agent, users can provision Enterprise users from LDAP to SAP StreamWork.
- In the Central Management Console (CMC) in the BI platform, administrators can create users and map them to Enterprise users.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- In the BI launch pad, users can create activities and view them in a browser, without creating an account or logging on to SAP StreamWork.
- In the BI launch pad, users can view and respond to SAP StreamWork feeds.

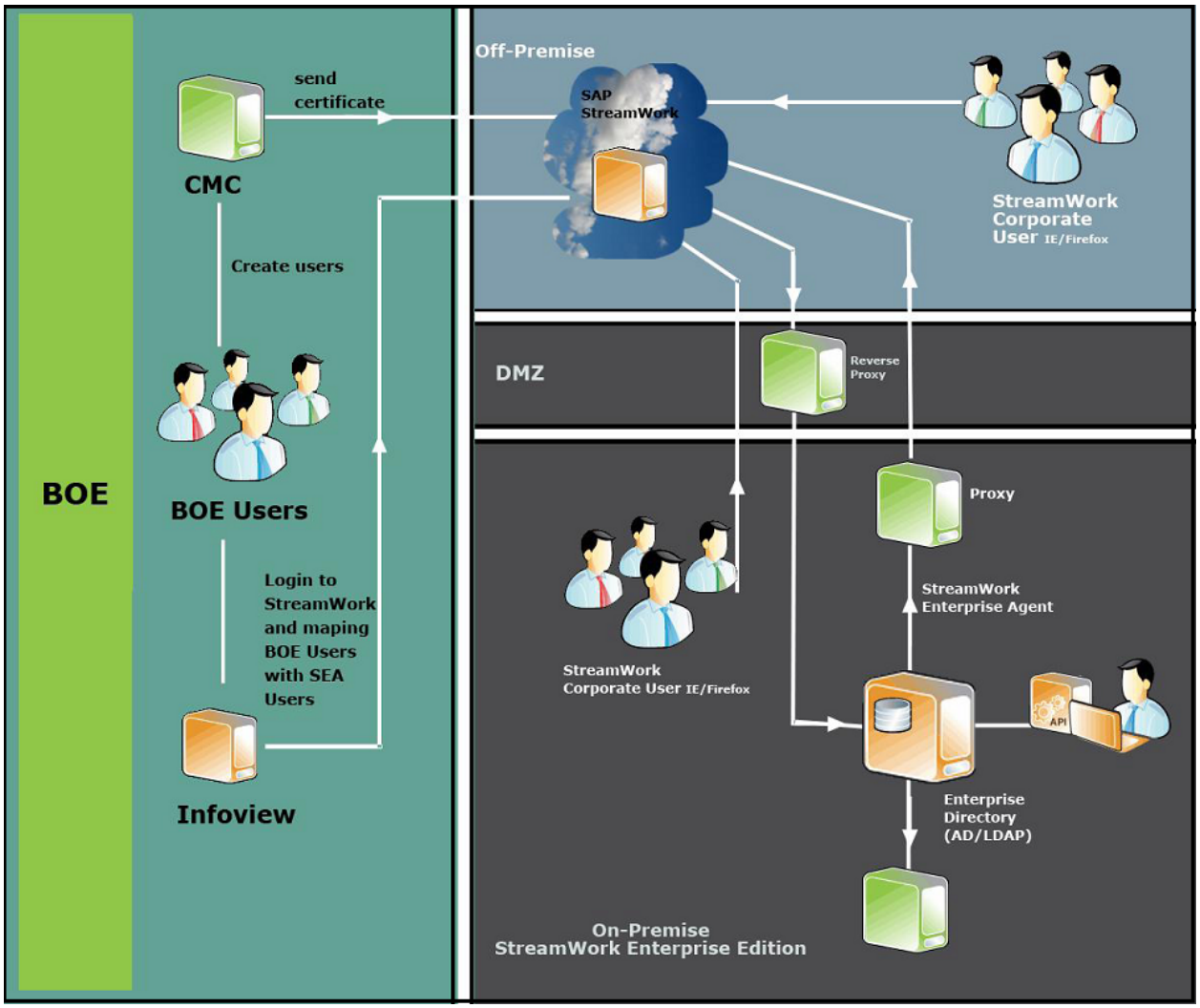


Figure 12: System landscape

18.1.3.8.4.2 Creating an OAuth Consumer Key for SAP StreamWork

Before you can create an OAuth Consumer Key, you must have administrator rights for the SAP StreamWork Enterprise organization.

1. In the SAP StreamWork administration console, on the *Admin* tab, select *SAML Trusted IDPs*, and log on to SAP StreamWork using an account designated as an Enterprise organization administrator.
2. Click *Register your identity provider*.
3. Select *Click here to create a new administrative OAuth application*, and accept the Terms of Use Agreement.
4. In the *Register a new Application OAuth application* window, perform the following actions:
   a. In the *Application Name* box, enter the name of the application instance to use in the integration.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This information identifies which application is needed to take action on behalf of a user—for example, to post SAP StreamWork feeds for a user. Users must be able to recognize this application name.

b. In the *Integration URL* box, enter the URL for the BI launch pad.

c. In the *Base64 X509 Certificate* box, enter the Base64 certificate value that was generated when SAP StreamWork was configured in the Central Management Console (CMC) in the BI platform.

   If you do not have the value, contact your external application administrator.

5. Click *Register*.
   The OAuth Consumer Key is generated. Make a note of the OAuth Consumer Key value for the BI platform administrator to use.
6. Click *Back* to display the SAML trusted identity providers.
7. In the *Register a new SAML Trusted Identity Provider* window, perform the following actions:

   a. In the *Display Name* box, enter a name for the BI platform deployment.
   This name will appear to users in SAP StreamWork.

   b. In the *IDP ID* box, enter the unique identity provider value that was created when SAP StreamWork was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

   c. In the *Base64 X509 Certificate* box, enter the Base64 certificate value that was generated when SAP StreamWork was configured in the BI platform.

   If you do not have the value, contact your external application administrator.

8. Click *Register*.

18.1.3.8.4.3 Adding SAP StreamWork to a BI workspace

SAP StreamWork is hidden and must be manually revealed in the list of BI launch pad modules that you can add to a BI workspace.

1. Locate `C:\BusinessObjects\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.PerformanceManagement\web\WEB-INF\lib\aasdk-ivdm_ext.jar\conf-syst\conf-syst\home-analyticlist.xml`.

   The file content should start with the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<CHOICE>
<!--<SW_ACTIVITIES NAME="$MSG_SW_ACTIVITIES$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC
$"/>-->
<!--SW_FEED NAME="$MSG_SW_FEED$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/-->
<HOMEINBOX NAME="$MSG_HOMEINBOX$" DESCRIPTION="$MSG_HOMEINBOXDESC$"/>
<HOMEAPPLICATIONS NAME="$MSG_HOMEAPPLICATIONS$"
DESCRIPTION="$MSGHOMEAPPLICATIONSDESC$"/>
<HOMERECENTLYRUNDOCS NAME="$MSG_HOMERECENTLYRUNDOCS$"
DESCRIPTION="$MSG_HOMERECENTLYRUNDOCSDESC$"/>
<HOMERECENTDOCS NAME="$MSG_HOMERECENTDOCS$" DESCRIPTION="$MSG_HOMERECENTDOCSDESC
$"/>
<HOMEALERTS NAME="$MSG_ALERTNOTIFICATIONS$"
DESCRIPTION="$MSG_ALERTNOTIFICATIONSDESC$"/>
</CHOICE>
```

2. Remove the `!--` from the `SW_ACTIVITIES NAME=` and `SW_FEED NAME=` lines.
3. Restart the Tomcat server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP StreamWork Feed appears in the *BI Launch Pad Modules* list in the module library for BI workspaces, in the BI launch pad.

18.1.3.9 Managing Platform Search settings

In the *Applications* area of the CMC in the BI platform, you can specify system-level settings for the Platform Search application.

Related Information

Indexing Failure Listing [page 677]
Configuring Application Properties in the CMC [page 568]

18.1.3.9.1 Configuring Application Properties in the CMC

To configure the Platform Search application properties, complete the following steps:

1. Go to the *Applications* area of the CMC.
2. Select *Platform Search Application*.
3. Click *Manage* > *Properties*. The *Platform Search Application Properties* dialog box appears.
4. Configure the Platform Search settings:

Table 83:

Option	Description
Search Statistics	Platform Search offers the following search statistics: ○ Indexing Status: displays the status of the indexing process. ○ Number of indexed documents: displays the number of documents that are indexed. ○ Last indexed time stamp: displays the time stamp at which the document was last indexed.
Stop / Start Indexing	Start or Stop Indexing options enable you to start or stop the indexing process when you want to switch from continuous crawling to scheduled crawling, or for maintenance purposes. To stop indexing, click *Stop Indexing*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Default Index Locale	Platform Search uses the locale specified in the CMC for indexing all the non-localized BI documents. Once the document is localized the corresponding language analyzer is used for indexing. Search is based on the client's product locale, and the weighting is given to the client's product locale. You can configure the weighting in the CMC configuration properties.
Crawling Frequency	You can index the entire BI platform repository by using the following options: ○ Continuous crawling: With this option, indexing is continuous; the repository is indexed whenever an object is added, modified, or deleted. It allows you to view or work with the most up-to-date BI platform content. Set by default, continuous crawling updates the repository continuously with the actions that you perform. Continuous crawling works without user intervention, and reduces the time taken for indexing a document. ○ Scheduled crawling: With this option, indexing is based on the schedule set by the Schedule options. For more information about scheduling an object, refer to the *Scheduling an Object* section of Platform Search in the *SAP BusinessObjects Business Intelligence platform CMC Online Help*. **Note** ○ If you select *Scheduled Crawling* and set the *Recurrence* to an option other than *Now*, Platform Search displays the date and time stamp when the document is scheduled to be indexed next. ○ If you select *Scheduled Crawling*, then the *Start Indexing* button is enabled and the *Stop Indexing* button is disabled. ○ Once the scheduling is complete, the *Stop Indexing* button is disabled.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Index Location	The indexes are stored in shared folders in the following locations: ○ Master index location (indexes and speller): The master and speller indexes are stored in this location. During a search, the initial results are retrieved using the Master Index, and the speller indexes are used to retrieve suggestions. In a clustered BI platform deployment, this location should be on a shared file system that is accessible from all nodes in the cluster. ○ Persistent data location (Content stores): The content store is placed in this location. It is created from the master index location and remains synchronized with it. The content store is used to generate facets and process the initial hits generated from the Master Index location. In a clustered BI platform deployment, content stores are generated at every node. The persistent data location is the only index location that is affected by the clustered environment as it contains the content store folders. If a machine has a single search service, then there will be only one content store location. For example, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. However, in a clustered environment, if there are multiple search services, then each search service will have one content store location. For example, if you have two instances of a server running, then the content store locations would be as follows: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name 1>\ContentStores. ○ Non-persistent data location (Temporary files, Delta Indexes): In this location, the delta indexes are created and stored temporarily before being merged with the Master index. The indexes at this location are deleted once they are merged with the Master Index. In addition, surrogate files (output of the extractors) are created in this location and stored temporarily until they are converted into delta indexes. **Note** ○ Master index location must be a shared location. ○ You need to click *Stop Indexing* to modify the index location. ○ If you modify an index location, copy the content to a new location, or the existing index information will be lost.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description

Level of indexing	You can tune the search content by setting the level of indexing in the following ways:
	○ Platform Metadata: An index is created only for the platform metadata information such as titles, keywords, and descriptions of the documents. By default, this option is selected.
	○ Platform and Document Metadata: This index includes the platform metadata as well as the document metadata. The document metadata includes the creation date, modification date, and name of the author.
	○ Full Content: This index includes the platform metadata, document metadata, and other content such as:
	  ○ The actual content in the document
	  ○ The content of prompts and LOVs
	  ○ Charts, graphs, and labels
	Note
	Full content indexing is not supported for Analysis Office and Lumira documents. Only metadata indexing is supported for Analysis Office and Lumira documents.
	Note
	When you modify the level of indexing, the indexing is initialized for the entire BI platform repository refresh.

Content Types	You can select the following content types for indexing: ○ Crystal Reports ○ Web Intelligence ○ Universe ○ BI Workspace ○ Analysis Office ○ Lumira ○ Microsoft PowerPoint ○ Adobe Acrobat ○ Rich Text ○ Text ○ Microsoft Word ○ Microsoft Excel The content type filter does not apply for platform metadata indexing. Regardless of the content types you select, platform metadata indexing happens for all the supported object types and the search results in BI launch pad returns all the objects for the keyword related to platform metadata. The content type filter is relevant for document metadata indexing (document author, document header, document footer, and so on) and content indexing (graphs , charts , table with a report). Based on the level of indexing and content types you select, platform search indexes the document metadata and content for the selected objects types from the repository and only those objects appear in the BI launch pad search results, when searching for keyword related to document metadata and content.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Rebuild index	This option deletes the existing index and re-indexes the entire repository. You can select the *Rebuild index* option whether indexing is running or stopped. The existing index is deleted when you save your changes to the properties page. However, if indexing is currently stopped, the index does not start rebuilding until you restart indexing. If you do not want Platform Search to re-index the documents, clear the *Rebuild index* option before clicking *Start Indexing*.
Documents Excluded from Indexing	The *Documents Excluded from Indexing* option excludes documents from indexing. For example, you may not want extremely large Crystal reports to be made searchable to ensure the report application server resources are not overloaded. Similarly, you may not want publications with hundreds of personalized reports to be indexed. By excluding particular documents, you can prevent them from being accessed by Platform Search. It is important to note that if a document is already indexed before it is put into this group, the document may still be searchable. To ensure that documents in the *Documents Excluded from Indexing* group are not searchable, you must rebuild the index. By default, only the Administrator account has full control of the *Documents Excluded from Indexing* option. Other users with the following rights can only add documents to the *Documents Excluded from Indexing* group: ○ View and edit rights on the category ○ Edit the document directly

5. Click *Save & Close*.

> **Note**
>
> If a user does not select the *Rebuild Index* option and changes the level of indexing or selects or deselects extractors, then the index is incrementally updated without deleting the existing index.

18.1.3.10 Configuring BEx Web Integration

BEx Web applications are Web-based applications from the Business Explorer (BEx) of SAP Business Warehouse (BW) for data analysis, reporting, and analytical applications on the Web.

The Business Explorer is the SAP NetWeaver Business Intelligence suite, which provides flexible reporting and analysis tools for strategic analyses and decision-making support. These tools include query, reporting, and analysis functions. As an employee with access rights, you can evaluate historical or current data at various levels of detail and from different perspectives, both on the Web and in Microsoft Excel.

Users access the data from the SAP NetWeaver Portal or from the BI launch pad of SAP BI platform. Authors of BEx Web applications can execute the Web applications directly in the BI launch pad from BEx Web Application Designer.

To integrate BEx Web applications into the BI platform, perform the following configuration steps:

1. Set up a server for the BEx Web applications in the Central Management Console (CMC).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

You can use either a general or standalone server for the BEx Web applications.

> **Tip**
>
> We recommend setting up a standalone server for the BEx Web applications, as the general server is normally used by many other services.

2. Configure the server settings.
3. Check the connection to the BW system.
4. To ensure that authors can run BEx Web applications directly in the BI launch pad from BEx Web Application Designer, make the relevant settings in the *Connected Portals* table (**RSPOR_T_PORTAL**) in the BW system.

After the configuration of the BI platform server, users can open BEx Web applications in the BI launch pad. They can navigate in the data here and save the BEx Web applications as bookmarks in the web browser favorites.

> **Restriction**
>
> Integration is supported as of the following SAP NetWeaver releases:
>
> SAP NetWeaver 7.0 Enhancement Package 1 Support Package Stack 8
> SAP NetWeaver 7.3 Support Package Stack 1
>
> Because the SAP NetWeaver Java stack is not required for this integration, the following restrictions apply:
>
> Information Broadcasting is not supported.
> Because the portal and Knowledge Management of SAP NetWeaver are not needed, document integration and the use of portal motives are not supported in the BEx Web applications.
> The *Report* Web item is not supported. We recommend that you use SAP Crystal Reports for formatted reporting.
> To create print versions of BEx Web applications, the Export Library for SAP Business Explorer is used. Adobe Document Services (ADS) are not available.
> The BEx Web applications that are integrated into the BI platform can contain only data sources that are stored in the BW master system. In system administration, you define which system is configured as the BW master system in the BI platform.
> Single sign-on between the BI platform and the SAP NetWeaver BW system is not enabled. For each BI platform session, BEx Web applications users are requested to log on to the corresponding BW master system.
> Report-report interface from and to BEx Web applications is not supported. Corresponding commands won't be executed.
> Dashboards based on BEx queries or query views and created with SAP BusinessObjects Dashboards are not supported.

For more information about the features of BEx Web applications, see the SAP Help Portal at http://help.sap.com: *SAP NetWeaver 7.3* > *SAP NetWeaver Library: Function-Oriented View* > *Business Warehouse* > *SAP Business Explorer* > *BEx Web* > *Analysis & Reporting: BEx Web Applications*.

For more information about accessing and saving BEx Web applications in the BI launch pad, see the *BI Launch Pad User Guide* at http://help.sap.com.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Starting a Server for BEx Web Applications [page 574]
Starting a Standalone Server for BEx Web Applications [page 574]
Configuring Server Settings [page 574]
Checking Connection to BW System [page 575]
Configuring a Connection Between BEx Web Application Designer and the BI platform [page 576]

18.1.3.10.1 Starting a Server for BEx Web Applications

Before you can perform this task, the Adaptive Processing Server must be in a Stopped state.

1. Log on to the Central Management Console (CMC).
2. Choose *Servers*.
3. Expand the *Service Categories* node, and choose *Analysis Services*.
4. Select *Adaptive Processing Server*, and choose *Select Services* in the context menu.
5. Move *BEx Web Applications Service* from the *Available Services* list to the Services list on the right side.
6. Restart the BEx Web Applications Service by restarting the Adaptive Processing Server.

18.1.3.10.2 Starting a Standalone Server for BEx Web Applications

1. Log on to the Central Management Console (CMC).
2. Choose *Servers*.
3. Expand the *Service Categories* node and choose *Analysis Services*.
4. Select the *Adaptive Processing Server* and choose *Clone Server* in the context menu.
5. Enter a name for the server (`AdaptiveProcessingServer` for example) and select the required node in the *Clone to Node* box.
6. Select the cloned server and choose *Select Services* in the context menu.
7. Select *BEx Web Applications Service* in the *Available Services* list and move it to the Services list on the right side.
8. Start the BEx Web Applications Service by starting the new Adaptive Processing Server.

18.1.3.10.3 Configuring Server Settings

1. Log on to the Central Management Console (CMC).
2. Choose *Servers*.
3. Expand the *Service Categories* node and choose *Analysis Services*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Select the server that hosts the BEx Web Applications Service and choose *Properties* in the context menu.
5. Under the *BEx Web Applications Service Configuration* in the *BEx Web Applications Service* area, make the following settings:
   a. Check (and change if necessary) the maximum number of client sessions.
   b. Under *SAP BW Master System*, enter the name of the OLAP connection to the BW system that you created in the BI platform. The default name is *SAP_BW*.
   c. Enter the name of the *JCo Server RFC Destination* that you entered in the BW system under *Configuration of RFC Connections* (transaction code **sm59**).
   d. Enter the name of the *JCo Server Gateway Host* that you defined in the BW system under *Configuration of RFC Connections* (transaction code **sm59**).
   e. Enter the name of the *JCo Server Gateway Service* that you defined in the BW system under *Configuration of RFC Connections* (transaction code **sm59**).
   f. Check (and change if necessary) the *JCo Server Connection Count*.
6. Choose *Save & Close*.
7. Select the server that hosts the BEx Web Applications Service and choose *Restart Server* in the context menu.

   To apply the selected settings, you have to restart the server.

> **Note**
>
> Before you restart the server, the RFC destination in the ABAP system must have been created.

Related Information

Creating an RFC destination in the ABAP System [page 576]

18.1.3.10.4 Checking Connection to BW System

1. Log on to the Central Management Console (CMC).
2. Choose *OLAP Connections*.
3. Check whether a connection has been established to the BW system. If not, click the *New connection* button to set one up. The default name of the connection is **SAP_BW**. You can also enter a different name.
4. Make sure that you have selected *Pre-defined* under *Authentication* and have made the required entries for user and password.

> **Note**
>
> This user account is required for the JCo server RFC destination, which allows the integration of BEx Web Application Designer, the BW system, and the BI platform.

> **Tip**
>
> To make the connection secure, make sure that only administrators have access rights to it.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. To do this, right-click the connection to the BW system (default name **SAP_BW**) and choose *User Security*.
2. Make the required security settings and give access rights only to administrators if possible.

18.1.3.10.5 Configuring a Connection Between BEx Web Application Designer and the BI platform

To ensure that authors can run BEx Web applications directly in the BI launch pad from BEx Web Application Designer, you need to make the relevant settings in the *Connected Portals* table (**RSPOR_T_PORTAL**) in the BW system.

1. In the BW system, call transaction **SM30** (*Table View Maintenance*).
2. Under *Table/View*, enter **RSPOR_T_PORTAL**.
3. Choose *Maintain*.
4. To create a new entry, choose *New Entries*.
5. Make the following settings:
   a. To ensure integration between the BW system and the BI platform, you have to create an RFC destination in transaction **SM59**. Enter this RFC destination under *Destination*.
   b. Select *Standard Portal*. This ensures that Web applications in Web Application Designer are always called in the BI platform.
   c. Under *URL Prefix*, enter the URL to the BI platform Web Application Container Server (WACS), including the protocol, host name and port, **http://<wacs><domain>:<port>** for example.
   d. Under *Platform*, select *BOE*.
   e. Select *Use SAP Export Lib (PDF)* if you want the Export Library for SAP Business Explorer to be activated, thus allowing PDF, PostScript and PCL files to be exported from BEx Web applications.
6. Save your entries.

Related Information

Creating an RFC destination in the ABAP System [page 576]

18.1.3.10.5.1 Creating an RFC destination in the ABAP System

To integrate the BW system and the BI platform, you need an RFC destination. This RFC destination allows the BW system and the BI platform to communicate with one another.

1. Call *Configuration of RFC Connections* (transaction code**SM59**).
2. Choose *Create*.
3. Maintain the RFC destination:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

a. Enter a name for the RFC destination.
b. Select *T for TCP/IP connection* as the connection type.
c. Enter a description.

   You can maintain the description of the RFC destination language dependently.
d. Under *Technical Settings*, select *Registered Server Program* as the activation type.
e. Under *Technical Settings*, enter the program ID.

   The program ID must be identical to the program ID (JCo Server RFC Destination) that you specified when creating the destination for this BW system in the BI platform server.
f. Under *Technical Settings* under *Gateway Options*, enter the gateway host and the gateway service that the BI platform server uses to communicate with the BW system.

4. On the *Logon & Security* tab page, activate the *Send SAP Logon Ticket* option.
5. Save your entries.

Related Information

Configuring Server Settings [page 574]

18.1.3.11 Configuring SAP HANA single sign-on

In the *Applications* area of the CMC in the BI platform, you can configure single sign-on (SSO) for SAP HANA database connections. SSO is implemented using SAML (Security Assertion Markup Language).

Once you have established a BI platform session, you will be able to generate a SAML ticket that can be used to log in to SAP HANA without requiring the user to provide a password.

This is the basic workflow involved in connecting to SAP HANA data sources:

1. An administrator configures a trust between SAP HANA and the BI platform in the CMC.
2. A user logs into the BI platform with any of the supported authentication providers.
3. Provided that the SAP HANA and BI platform user IDs match, the BI platform is able to generate a SAML assertion that SAP HANA can accept to establish a connection for the current user. The user ID that is passed to SAP HANA is the BI platform user ID for the user that logged in.
4. A BI platform client application creates an SAP HANA connection.

> **Note**
>
> Before configuring SAP HANA single sign-on with SAML, you must configure SSL on the SAP HANA machine. See your SAP HANA documentation for details.

18.1.3.11.1 To create an SAP HANA connection

1. Get the relevant SAP HANA database parameters.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

a. Open the SAP HANA Studio application.
b. Open the properties page for your system, and find the URL for the database connection.
c. Record the host machine name and the port number.

   You'll need this information in step 2.

2. Configure an SAP HANA connection in the BI platform.
   a. Go to the *Applications* area of the CMC and double-click *HANA Authentication*.
   b. In the *HANA Authentication* dialog box, click the *Create a connection* button.
      The *Create HANA Authentication Connection* dialog box opens.
   c. Enter the host machine name and port number that you recorded in step 1.
   d. In the *Unique Identity Provider ID* field, specify a value that will be used for your BI platform deployment.
   e. Click *Generate*.
      A certificate is created in the *Identity Provider Base64 Certificate* box.
3. Configure your SAP HANA deployment.
   a. Using the SAP HANA Studio application, right-click the SAP HANA system, and click *Properties*.
   b. Select *SAML Configuration*.
   c. Click *Add*.
   d. In the *Create SAML Identity Provider* dialog box, select *Read from Certificate*.
   e. Click *Open File* to populate the DN values.
   f. Click *OK*.
   g. Restart SAP HANA.
4. Test the SAP HANA configuration.
   a. Go to the *Applications* area of the CMC and double-click *HANA Authentication*.
   b. In the *HANA Authentication* dialog box, open the connection you created in step 2.
      The *Edit HANA Authentication Connection* dialog box opens.
   c. Under *Test the connection for this user*, enter a user name and click the *Test Connection* button to verify that your connection settings are valid.

      For example, enter the user name **`Administrator`**. If the settings are not valid, an error message is displayed. You can try these troubleshooting steps:

      - Ensure that no other certificate in the `trust.pem` file contains a Subject or Issuer with the same CN property value. To see the components of the certificate, search the internet for "x509 certificate decoder" to find a certificate decoder.
      - Try these commands to check the HANA-side configuration:

```
select * from "SAML_PROVIDERS"
select user_name, is_saml_enabled from users where user_name =
'<UserName>'
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

      - If a SAML authentication error is displayed while configuring SSO to SAP HANA, try these steps:
        1. In the `indexserver.ini` file, set the parameter `sslCreateSelfSignedCertificate` to **`false`**.
        2. In the same file, set the parameters `sslKeyStore` and `sslTrustStore` to use absolute paths.
        3. Regenerate the `key.pem` and `trust.pem` files.

If the `key.pem` file does not exist in the `.ssl` directory, then SAP HANA was not configured correctly to use SSL.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.1.3.11.2 SAP HANA connection settings

The table below summarizes the settings available in the CMC for configuring SAP HANA connections.

Table 84:

Setting	Description
HANA Hostname	Provide the name of your SAP HANA host.
HANA Port	Provide the port number for your SAP HANA host.
Unique Identity Provider ID	A unique name within a given HANA installation. The HANA installation will accept properly signed tickets from this identity provider name for logons.
Identity Provider Base64 Certificate	When you click *Generate*, a certificate is created in the *Identity Provider Base64 Certificate* field. Copy this certificate to the `trust.pem` file in your SAP HANA deployment. This certificate establishes the trust relationship between SAP HANA and the BI platform. The external identity provider itself is identified with an X509 certificate, which is used to sign all identity assertions. The certificate must be Base64 encoded.

18.1.3.12 Managing SAP Lumira Settings

From the "Applications" area of CMC, you can manage rights related to data acquisition and content sharing functionality of SAP Lumira for each user or user group.

To manage rights for SAP Lumira, perform the following steps:

1. From the CMC Home page, select *Applications* > *SAP Lumira* > *User Security*.
2. Select the user or group you want to set rights for.
3. Select *Assign security*.
4. Select *Advanced*.
5. Select *Add/Remove rights*.
6. Define the rights that the user needs to have for SAP Lumira.
7. Click *Apply*.

18.2 Managing applications through BOE.war properties

18.2.1 The BOE war file

You can modify settings for BI platform web applications by overwriting default properties for the BOE.war file. This file is deployed on the machine hosting the web application server. For detailed information on how the file is deployed see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide.*

The properties contained in the BOE.war file control specifications for default login behavior, default authentication methods, settings for single sign-on. There two types of properties you can specify:

- Global properties - these properties affect all the web applications contained in the BOE.war file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Application-specific properties - property settings that affect only a specific web application.

To modify any of the default properties, use the custom configuration directory to save new settings for either global or application-specific properties. By default, the directory is located at: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Do not modify the properties in the `config\default` directory.

> **Note**
>
> On some web application servers such as the Tomcat version bundled with the BI platform, you can access the BOE.war directly. In this scenario, you can set custom settings directly without undeploying the WAR file. When you cannot directly access the deployed web applications, you must undeploy, customize, and then redeploy the file. For more information, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

18.2.1.1 Global BOE.war properties

The following table lists the settings included in the default `global.properties` file for BOE.war.

To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Default values	Description
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Enables or disables persistent cookies on the web application logon page.
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Specifies what authentication method to use with SiteMinder. Only options are secLDAP and secwinAD.
`siteminder.enabled`	`siteminder.enabled=false`	Enables and disables authentication with SiteMinder.
`sso.enabled`	`sso.enabled=false`	Enables and disables single sign-on (SSO) to BI platform.
`sso.sap.primary`	`sso.sap.primary=false`	Set to `true` if you want to use SAP SSO as the application's primary single sign-on mechanism. Only applies to cases where both SAP and SiteMinder SSO are used.
`max.tree.children.threshold`	`max.tree.children.threshold=200`	Specifies the threshold at which the tree list control will not display all the nodes, and will instead display a "too many children" message.
`trusted.auth.shared.secret`	None	Specifies the session variable name used to retrieve the secret for Trusted Authentication. Only applies if using the web session to pass the shared secret.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Default values	Description
trusted.auth.user.param	None	Specifies the variable used to retrieve the user name for Trusted Authentication, and can be set to one of the following values: • Header • URL Parameter • Cookie • Session
trusted.auth.user.retrieval	None	Specifies the method used to retrieve the username for Trusted Authentication., and can be set to one of the following values: • "REMOTE_USER" • "HTTP_HEADER" • "COOKIE" • "QUERY_STRING" • "WEB_SESSION" • "USER_PRINCIPAL" Set to empty to disable Trusted Authentication.
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	Enables and disables dynamic binding of aliases to existing user accounts. If property is set to true, Trusted authentication uses alias binding to authenticate users to the BI platform. With alias binding, your application server can work as a SAML service provider therefore enabling Trusted Authentication to provide SAML SSO to the system. If set to false, Trusted Authentication uses name matching to authenticate users.
vintela.enabled	vintela.enabled=false idm.realm=YOUR_REALM idm.princ=YOUR_PRINCIPAL idm.allowUnsecured=true idm.allowNTLM=false idm.logger.name=simple idm.logger.props=error-log.properties	Used to enable or disable Vintela settings for Windows AD authentication.
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	Specifies whether or not to display the warning dialog with the message indicating that the current session will expire soon in the CMC.
pinger.showWarningDialog.bilaunchpad	pinger.showWarningDialog.bilaunchpad=true	Specifies whether or not to display the warning dialog with the message indicating that the current session will expire soon in BI launch pad.
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	Specifies how often a web server request should be sent while the session expiry warning message is displayed. This is important for synchronizing the warning dialog across applications.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Default values	Description
pinger.warningPeriod.lengthInMinutes	pinger.warningPeriod.lengthInMinutes=5	Specifies how long prior to session expiry the warning should be displayed.
logoff.on.websession.expiry	logoff.on.websession.expiry=true	Specifies if all application sessions log off when the web session expires.
pinger.enabled	pinger.enabled=true	Enables or disables the session expiry warning messaging mechanism.
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	Specifies the maximum number of cached Java connections.
httpproxy.username	httpproxy.username=myusername	Specifices the username to log on to the HTTP proxy server.
httpproxy.password	httpproxy.password=mypassword	Specifices the password to log on to the HTTP proxy server.
logon.embed.secret	None	A shared secret between a portal that embeds BI platform applications and the BI platform application server, which is used to determine whether BI platform applications can be safely embedded in other pages.
logon.embed.timeout	logon.embed.timeout=300	The number of seconds after which BI platform applications such as BI launch pad will reject being embedded into a portal. Ensure that the system clocks on the BI platform web server and the portal server machines are within this number of seconds of each other.
iview.autologoff	iview.autologoff=true	Set to `true` to enable immediate autologoff for iViews in SAP NetWeaver technology platform.
pinger.showWarningDialog	pinger.showWarningDialog=true	Specifies whether or not to display the warning dialog with the message indicating that the current session will expire soon. Does not apply to the CMC & BI launch pad.
ure.request.queue.timeout.seconds	ure.request.queue.timeout.seconds=20	The number of seconds a request will wait for expected previous requests before timing out When users perform navigation or folder expansion actions in the tree list control in the BI launch pad, AJAX requests are queued for those actions. The user interface waits for these requests to complete before relinquishing control to the user. This setting determines the number of seconds that the user interface will wait for each request, if unexpected delays occur in the back-end query.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.2.1.2 BI launch pad properties

The following table lists the settings included in the default `bilaunchpad.properties` file for the BOE war file. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Description
`app.name`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name=BI launch pad`
`app.name.short`	Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: `app.name.short=BI launch pad`
`app.url.name`	Specifies the URL name of the application, preceded by the "/"" character. Default: `app.url.name=/BI`
`authentication.default`	Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting: **Authentication** / **Setting value** Enterprise / `secEnterprise` LDAP / `secLDAP` Windows AD / `secWinAD` SAP / `secSAPR3` PeopleSoft / `secpsenterprise` JD Edwards / `secPSE1` Siebel / `secSiebel7` Oracles EBS / `secOraApps` Default: `authentication.default=secEnterprise`
`authentication.visible`	Specifies if users logging into BI launch pad have the option to view and change the authentication method. Default: `authentication.visible=false`
`cms.default`	Specifies the default CMS name. Default: `cms.default=[name of host machine]`
`cms.visible`	Specifies if users logging into BI launch pad have the option to view and change the CMS name. Default: `cms.visible=true`
`dialogue.prompt.enabled`	Specifies if users should be prompted when navigating away from an input page in a dialog box. Default: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Specifies whether or not to enable token creation for the session after a user logs into BI launch pad. Token will be

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Description
	stored in a cookie. Default: `logontoken.enabled=false`
`SMTPFrom`	Enables or disables the *From* field when scheduling an object to a destination. Default: `SMTPFrom=true` When the value is set to `false` the *From* field will not be displayed and the system attempts to retrieve the *From* email value in the following order: 1. First, from the report default for a report object. 2. Second, from the email address on the user profile of the logged on user. 3. Lastly, from the Job server default.
`url.exit`	Specifies which URL to redirect users after terminating their BI launch pad session. This setting applies only to users who have logged into the application through an external verification process.
`disable.locale.preference`	Enables or disables the user from viewing and thus modifying the viewing local preferences for BI launch pad. Default: `disable.locale.preference=false`
`extlogon.allow.logoff`	Enables or disables automatically logging off user sessions once they have closed their BI launch pad session. Set to false if you want user sessions not to automatically terminate when users log off BI launch pad. Default: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Specifies whether to allow other pages to embed this application (as a frame) without passing a valid embed token. Default: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Specifies a comma-delimited list of SSO types to be enabled, and the order in which they are executed. An empty list indicates that the legacy ordering is to be used. If the list is specified, the legacy options will be ignored. Valid options: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO`, and `siteminder`. If none are desired, specify: `none`

18.2.1.3 OpenDocument properties

The following table lists the settings included in the default `opendocument.properties` file for the BOE war file. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>app.name</td><td>Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: app.name=SAP BusinessObjects OpenDocument</td></tr>
<tr><td>app.name.short</td><td>Specifies the display name of the application. The name appears on the web application title page and logon screen. Default: app.name.short=OpenDocument</td></tr>
<tr><td>authentication.default</td><td>Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting:<table><tr><th>Authentication</th><th>Setting value</th></tr><tr><td>Enterprise</td><td>secEnterprise</td></tr><tr><td>LDAP</td><td>secLDAP</td></tr><tr><td>Windows AD</td><td>secWinAD</td></tr><tr><td>SAP</td><td>secSAPR3</td></tr><tr><td>PeopleSoft</td><td>secpsenterprise</td></tr><tr><td>JD Edwards</td><td>secPSE1</td></tr><tr><td>Siebel</td><td>secSiebel7</td></tr><tr><td>Oracles EBS</td><td>secOraApps</td></tr></table>Default: authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Specifies if users logging into OpenDocument have the option to view and change the authentication method. Default: authentication.visible=false</td></tr>
<tr><td>cms.default</td><td>Specifies the default CMS name. Default: cms.default=[name of host machine]</td></tr>
<tr><td>cms.visible</td><td>Specifies if users logging into OpenDocument have the option to view and change the CMS name. Default: cms.visible=true</td></tr>
<tr><td>logontoken.enabled</td><td>Specifies whether or not to enable token creation for the session after a user logs into OpenDocument. The token will be stored in a cookie. Default: logontoken.enabled=false</td></tr>
<tr><td>extlogon.allow.logoff</td><td>Enables or disables automatically logging off user sessions once they have closed their OpenDocument session. Set to false if you want user sessions to not automatically terminate when users log off OpenDocument. Default: extlogon.allow.logoff=true</td></tr>
<tr><td>SAPLogonToken.enabled</td><td>Specifies whether or not to allow RESTful Web Service SAP logon tokens to authenticate to the BI platform. The SAP logon token is specified by the X-SAP-LogonToken value in the request header after a successful logon with the RESTful</td></tr>
</table>

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Setting	Description
	Web Service URL. Default: `SAPLogonToken.enabled=true`
`logon.allowInsecureEmbedding=false`	Specifies whether to allow other pages to embed this application (as a frame) without passing a valid embed token. Default: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Specifies a comma-delimited list of SSO types to be enabled, and the order in which they are executed. An empty list indicates that the legacy ordering is to be used. If the list is specified, the legacy options will be ignored. Valid options: `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO`, and `siteminder`. If none are desired, specify: `none`

18.2.1.4 CMC properties

The following table lists the settings included in the default `cmc.properties` file for BOE.war. To overwrite any of the settings, create a new file in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Setting	Description
`app.url.name`	Specifies the URL name of the application, preceded by the"/"" character. Default: `app.url.name=/CMC`
`authentication.default`	Specifies the default authentication method used to authenticate users into the application. You can use any of the following for this setting:

Authentication	Setting value
Enterprise	`secEnterprise`
LDAP	`secLDAP`
Windows AD	`secWinAD`
SAP	`secSAPR3`
PeopleSoft	`secpsenterprise`
JD Edwards	`secPSE1`
Siebel	`secSiebel7`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td></td><td><table><tr><th>Authentication</th><th>Setting value</th></tr><tr><td>Oracles EBS</td><td>secOraApps</td></tr></table>Default: authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Specifies if users logging into the CMC have the option to view and change the authentication method. Default: authentication.visible=false</td></tr>
<tr><td>cms.default</td><td>Specifies the default CMS name. Default: cms.default=[name of host machine]</td></tr>
<tr><td>cms.visible</td><td>Specifies if users logging into the CMC have the option to view and change the CMS name. Default: cms.visible=true</td></tr>
<tr><td>dialogue.prompt.enabled</td><td>Specifies if users should be prompted when navigating away from an input page in a dialog box. Default: dialogue.prompt.enabled=false</td></tr>
<tr><td>logontoken.enabled</td><td>Specifies whether or not to enable token creation for the session after a user logs into the CMC. The token will be stored in a cookie. Default: logontoken.enabled=false</td></tr>
<tr><td>SMTPFrom</td><td>Enables or disables the From field when scheduling an object to a destination. Default: SMTPFrom=true

When the value is set to false the From field will not be displayed and the system attempts to retrieve the From email value in the following order:

1. First, from the report default for a report object.
2. Second, from the email address on the user profile of the logged on user.
3. Lastly, from the Job server default.</td></tr>
</table>

18.3 Customizing BI launch pad and OpenDocument logon entry points

You can customize the logon page for BI launch pad and OpenDocument web applications. For example, you can customize the logon page to use a company logo or corporate style sheet, or you can create a customized logon page that enables trusted authentication.

To customize the logon page, modify the `custom.jsp` file stored in the BI launch pad and OpenDocument application areas of the `BOE.war` web application, and then redeploy the `BOE.war` web application to your BI platform system. Users access the custom logon entry point by navigating to a unique URL.

To work with these examples, you need to be familiar with deploying BI platform web applications. For more information, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.3.1 BI launch pad and OpenDocument file locations

The BI launch pad and OpenDocument web applications are packaged within the `BOE.war` web archive file. The location of the `BOE.war` archive is defined in the `BOE.properties` file.

The `BOE.properties` file is found here on Windows systems:

- **<BOE_INSTALL_DIR>**`\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

The `BOE.properties` file is found here on UNIX systems:

- **<BOE_INSTALL_DIR>**`/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

The following tables define the location of common files within the `BOE.war` web archive file for both the BI launch pad and OpenDocument applications.

Table 85: BI launch pad file locations

> **Note**
>
> The BI launch pad web application was formerly known as InfoView.

File type	Location
Custom logon script	`WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`
Directory for additional files	`WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`
Custom logon URL	`http://<servername>:<port>/BOE/BI/custom.jsp`

Table 86: OpenDocument file locations

File type	Location
Custom logon script	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp`
Directory for additional files	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources`
Custom logon URL	`http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp`

18.3.2 To define a custom logon page

You can customize the entry point to the BI platform logon page. For example, you can create a custom logon page that displays a company logo and uses a corporate style sheet.

Edit the `custom.jsp` file to customize the logon experience for your users, and place supporting files in the `noCacheCustomResources` folder.

This example shows how to create a custom logon page that redirects the user to the standard logon page.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Create a file that contains your custom logon code, and save it as `custom.js` in the `noCacheCustomResources` folder.

   This example defines a function that redirects the user to the standard logon page, `logon.faces`.

   ```
   function load() {window.location =  "logon.faces";}
   ```

2. Edit the `custom.jsp` file to customize the logon page.

   This example displays a welcome message and a hyperlink that calls the `load` method defined in the `custom.js` file.

   ```
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">

   <%@ page language=  "java" contentType=  "text/html;charset=utf-8"%>
   <html>
     <head> <title>Welcome</title>
     </head>
     <body>
       <script type=  "text/javascript" src=  "noCacheCustomResources/custom.js"></
   script>
       <p>Welcome to ABC corporation.</p>
       <a href= "javascript:load()">Enter</a>
     </body>
   </html>
   ```

3. Redeploy the `BOE.war` web application, and restart the web server.

18.3.3 To add trusted authentication at logon

To enable trusted authentication, set the trusted user as a session attribute in the `custom.jsp` file, and modify authentication settings in a copy of the `global.properties` file. The values of the custom copy of the `global.properties` file override the default values.

1. Edit the `custom.jsp` file to set a session attribute that defines the trusted user.

   ```
   request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
   ```

2. Create a custom copy of the `global.properties` file by copying `WEB-INF\config\default\global.properties` to `WEB-INF\config\custom\global.properties`.
3. Modify `WEB-INF\config\custom\global.properties` to enable Single Sign-on (SSO).

   ```
   sso.enabled=true
   ```

4. Modify `WEB-INF\config\custom\global.properties` to set trusted authentication parameters, including the trusted user session variable, and the shared secret.

   Replace `"..."` with the shared secret for your system.

   ```
   trusted.auth.user.param=TrustedUserAttribute
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.shared.secret="..."
   ```

   For more details, see the related topic on configuring trusted authentication for web applications.
5. Redeploy your web application, and restart the web server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. In the CMC, enable trusted authentication.

   On the *Authentication* tab, double-click *Enterprise*, and then select the check box *Trusted Authentication is enabled*.

Related Information

Enabling Trusted Authentication [page 206]
To configure Trusted Authentication for the web application [page 210]

18.4 Customizing application user interfaces

Some application user interfaces can be customized through the CMC.

In the Central Management Console, you can customize the appearance of some applications. For example, you can toggle user interface elements.

18.4.1 Web Intelligence

18.4.1.1 Customizing Web Intelligence interface elements by user group and folders

In CMC, you can customize the appearance of Web Intelligence interface elements for a user, depending on the user group they belong to and the folders containing Web Intelligence documents. For example, the entire toolbar or specific items in a toolbar, and customize access to specific document modes.

The Customization section contains the following section and tabs:

- Customized folders section
  On this section, you can select folders containing Web Intelligence documents for which you want to customize user interface and enable extensions.
- User Interface Elements tab
  On this tab, you can select individual interface elements to hide, such as a toolbar or tab, or their sub elements; for example a button command.
- Features tab
  On this tab, you can choose to hide all user interface elements related to a function; for example, Refresh.
- Extensions tab
  On this tab, you can enable Web Intelligence user interface extensions that you have created and deployed in your installation.

All interface elements appear by default. If you do not want specific elements to appear, you deselect them in the CMC as described in the "To customize the Web Intelligence interface appearance" section. All extension points

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

are disabled by default. If you want to make them available to users, you enable them in the CMC as described in the "Enabling Web Intelligence User Interface Extension Points for specific user groups" section.

> **Note**
>
> - The customization and the enabled extension points are applicable to all Web Intelligence application clients: HTML, Java Applet, and Rich Client.
> - It might happen that the customization and enabled extension points do not work on Web Intelligence Rich Client because of proxy or DNS configuration. To solve this problem, log in to the CMC with the IP address of the server instead of the server name when you customize Web Intelligence. This IP address will be used as a reference during customization.

The *Customization folders* section contains a folder named Default Folders, which is used to define default customization. You can choose folders for which you want to apply customization by clicking the *Add Folder* button. To avoid redefining the same customization for other folders, you can copy customization from one folder to another by using *Duplicate Customization* and *Paste Customization* options from the drop-down list. If you want to remove customization for a specific folder, you need to remove the folder that you have added by selecting the *Remove folder* option from the drop-down list.

> **Note**
>
> You cannot remove Default Folders from the *Customization folders* section.

The following rules are used to define customizations to apply to a user:

- If the user belongs to different groups, only the customization defined to the group whose ID is lower applies. The customization defined for the other groups containing the user does not apply.
- For nested folder structure, the immediate parent folder of the document that has been added in the list of customized folders define customizations for the document for user interface elements, features, and extensions.
- The customization defined for Default Folders apply for the documents stored in Personal Documents and Inboxes, and for documents for which the parent folder is not customized.
- The customization defined for user interface elements have priority over customization defined for features as features is only a shortcut to enable all user interface elements.

Related Information

Enabling Web Intelligence User Interface Extension Points for specific user groups [page 602]
To customize the Web Intelligence interface appearance [page 601]

18.4.1.1.1 User Interface Elements tab

Some of the interface elements that you can customize are identified in the diagrams in the subsequent subsections. Use the following table to identify the element items in the diagrams.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 87:

User Interface Element item	Sub-element item	Description	Number in diagram
Splash screen		The screen that appears when a user opens Web Intelligence.	
Application Contextual Menu		The menu that appears when a user right-clicks in the Web Intelligence screen.	1
	Application mode	The application mode change option in the Application Contextual Menu.	1a
	Filter Bar	The Filter Bar option in the Application Contextual Menu.	1b
	Outline	The Outline option in the Application Contextual Menu.	1c
	Formula Bar	The Formula Bar option in the Application Contextual Menu.	1d
	Side Panel	The Side Panel option in the Application Contextual Menu.	1e
	Report Tabs	The Report Tabs option in the Application Contextual Menu.	1f
	Status Bar	The Status Bar option in the Application Contextual Menu.	1g
Side Panel		The Side Panel next to the report panel that allows users access to various information tabs.	2
	Document Summary	The Document Summary tab in the Side Panel.	2a
	Navigation Map	The Navigation Map (called Report Map in the HTML interface) tab in the Side Panel.	2b
	Input Controls	The Input Controls tab in the Side Panel.	2c
	User Prompt Input	The User Prompt Input tab in the Side Panel.	2d
	Available Objects	The Available Objects tab in the Side Panel.	2e
	Document Structure and Filters	The Document Structure and Filters tab in the Side Panel.	2f
	Web Service Publisher	The Web Service Publisher tab in the Side Panel.	2g
	Data	The Data tab in the Side Panel.	2h
Status Bar		The Status Bar, where the user sees information on document action statuses and can perform zoom, page navigation, and formula bar activation tasks.	3
	Report dropdown list	The Report dropdown list in the Status Bar.	3a
	Printing status icon	The Printing status icon list in the Status Bar.	3b
	Track data changes	The Track data changes status in the Status Bar.	3c
	Page Navigation	The Page Navigation bar in the Status Bar.	3d
	Pagination Mode	The Pagination Mode buttons in the Status Bar.	3e
	Zoom List	The Zoom percentage dropdown list in the Status Bar.	3f
	Zoom Slider	The Zoom Slider bar in the Status Bar.	3g

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

User Interface Element item	Sub-element item	Description	Number in diagram
	Workspace Status	The Workspace Status indicator in the Status Bar. **Note** The Workspace Status indicator ( ) appears between the Zoom Slider and the Last Refresh Date if a problem occurs in the workspace.	Not shown
	Last Refresh Date	The document refresh date in the Status Bar.	3i
	Connection Status	The Web Intelligence Rich Client Connection Status in the Status Bar.	3j
Report Zone		The report zone in Web Intelligence.	4
	Report Tabs	The report tabs in the report zone.	4a
	Bi-directional Page Scrolling	The bi-directional page scrolling feature in the lower corner of the report zone page.	4b
	Formula Bar	The formula bar at the top of the report zone.	4c
Reading Mode Toolbar		The toolbars displayed in Reading mode.	5
	Web Intelligence dropdown list	The Web Intelligence dropdown list in the Reading mode.	5a
	File Group	The File Group toolbar in the Reading mode.	5b
	Standard Actions Group	The Standard Actions Group toolbar in the Reading mode.	5c
	Analysis Group	The Analysis Group toolbar in the Reading mode.	5d
Design Mode Toolbar		The toolbars and tabs displayed in the Design mode.	6
	File tab	The File tab in the Reading mode.	6a
	Properties tab	The Properties tab in the Reading mode.	6b
	Standard Actions Group	The Standard Actions Group toolbar in the Reading mode.	6c
	Report Elements tab	The Report Elements tab in the Reading mode.	6d
	Format tab	The Format tab in the Reading mode.	6e
	Data Access tab	The Data Access tab in the Reading mode.	6f
	Analysis tab	The Analysis tab in the Reading mode.	6g
	Page Setup tab	The Page Setup tab in the Reading mode.	6h
Initial Toolbar		The initial toolbars that appear when a user opens the Web Intelligence application.	7
	Web Intelligence dropdown list	The Web Intelligence dropdown list in the initial toolbar.	7a
	File Group	The File Group toolbar in the initial toolbar.	7b

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

User Interface Element item	Sub-element item	Description	Number in diagram
Application Control Toolbar		The Application Control Toolbar that appears in the upper toolbar of Web Intelligence.	8
	Application mode buttons	The application mode buttons (Reading, Design, and Data) in the upper toolbar of Web Intelligence.	8a
	Tools	The Tools icon in the upper toolbar of Web Intelligence.	8b
	Help	The Help icon in the upper toolbar of Web Intelligence.	8c
	Close	The Close icon in the upper toolbar of Web Intelligence.	8d
Shortcuts		Keyboard shortcuts; for example, CTRL + N or CTRL + S.	Not shown

Splash Screen

In the CMC Users and Groups Customization, you can choose to hide the Web Intelligence splash screen that appears. The following image shows the splash screen that appears by default when a user opens Web Intelligence.

Figure 13: Splash Screen (English example)

Application Contextual Menu

The following diagrams show the items that can be hidden in the right-click contextual menu.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

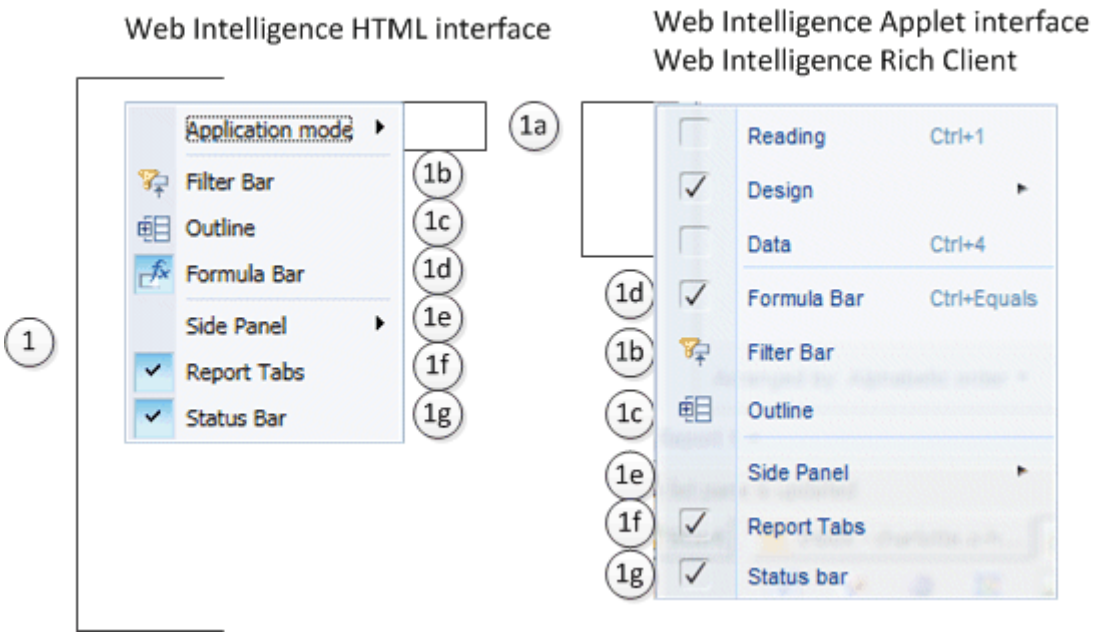
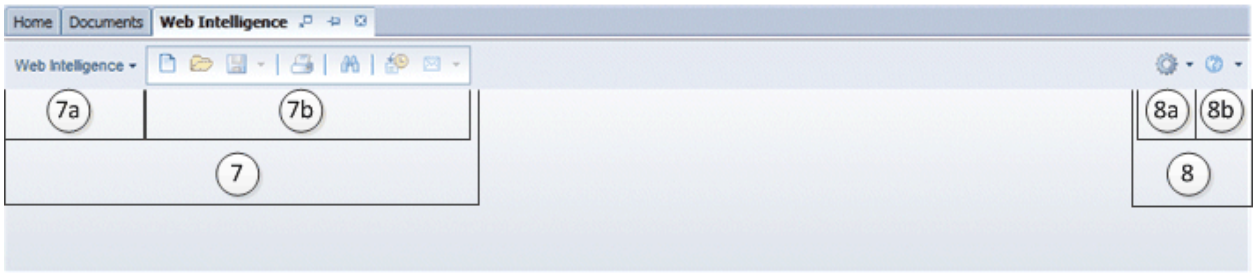


Figure 14: Application Contextual Menu (English example)

Initial Toolbar

The following diagrams show the items that can be hidden in the toolbars that appear in Web Intelligence when no document is open.

Web Intelligence Applet interface
Web Intelligence Rich Client



Web Intelligence HTML interface

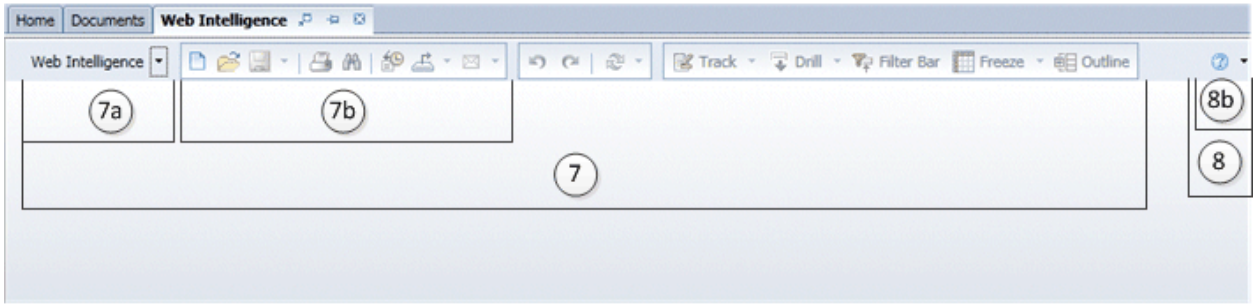


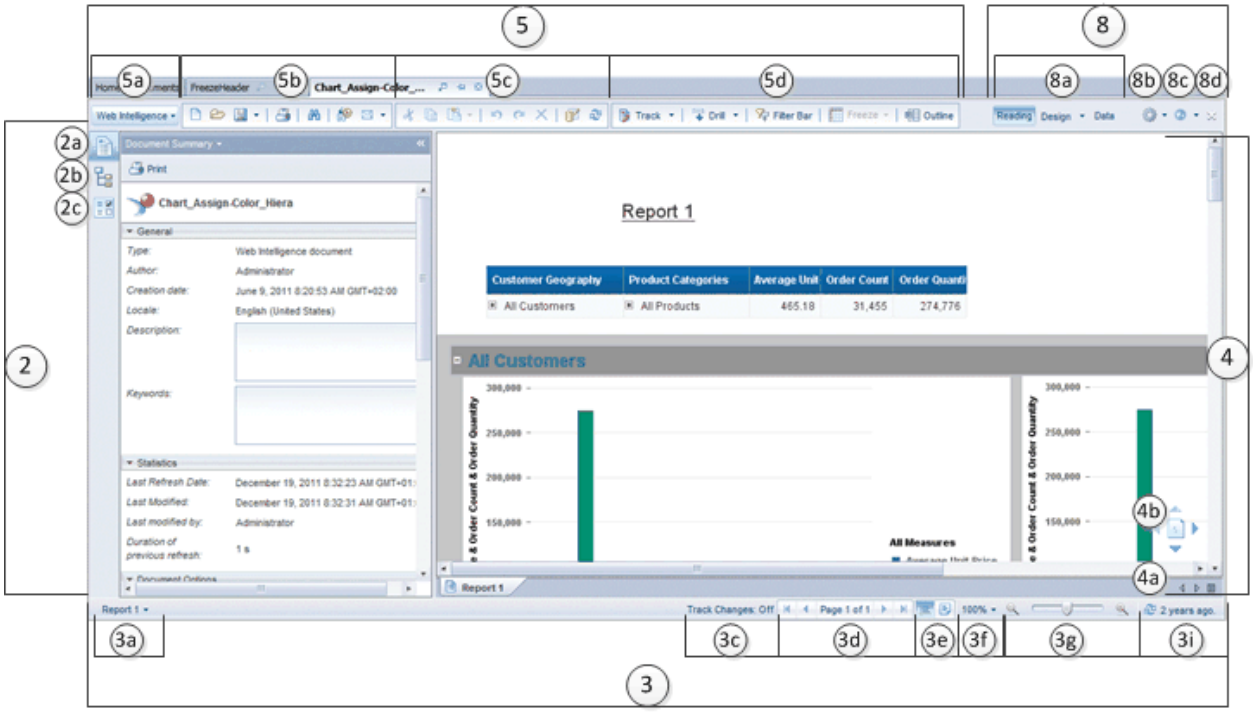
Figure 15: Initial Toolbar (English example)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

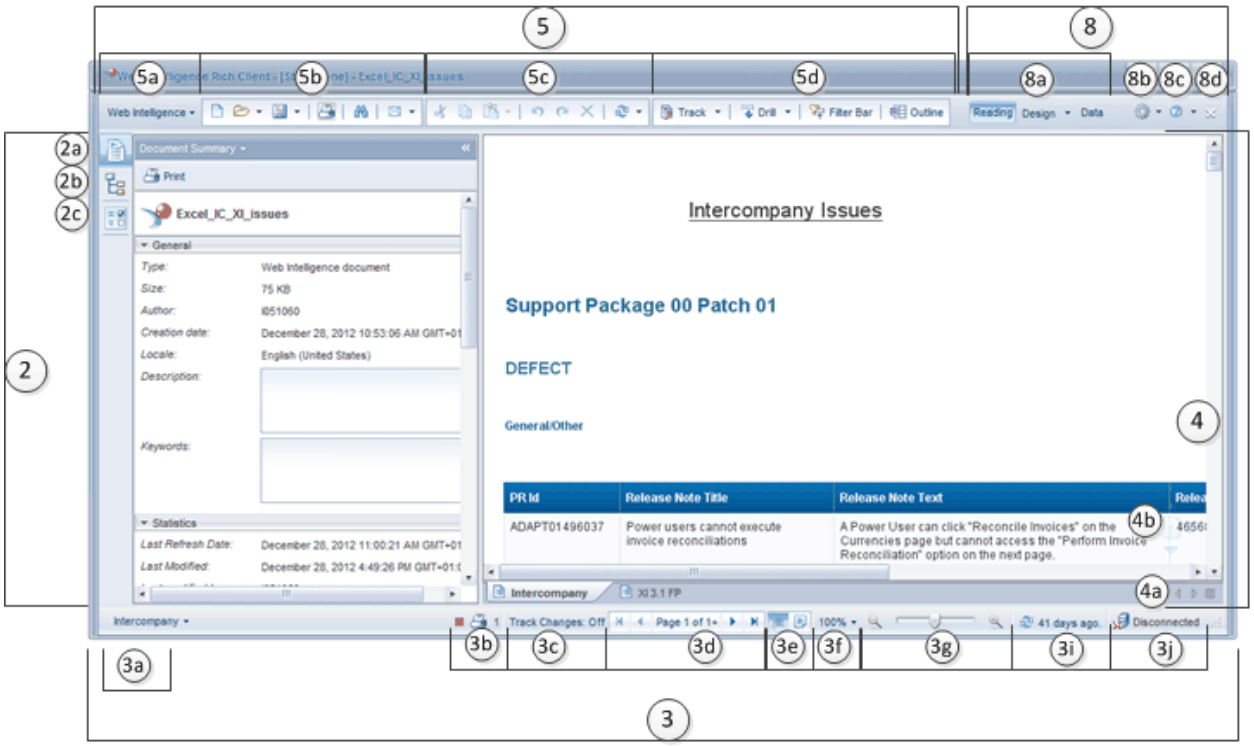
Reading Mode

The following diagrams show the items that can be hidden in the Web Intelligence Reading mode.

Web Intelligence Applet interface



Web Intelligence Rich Client



© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Web Intelligence HTML interface

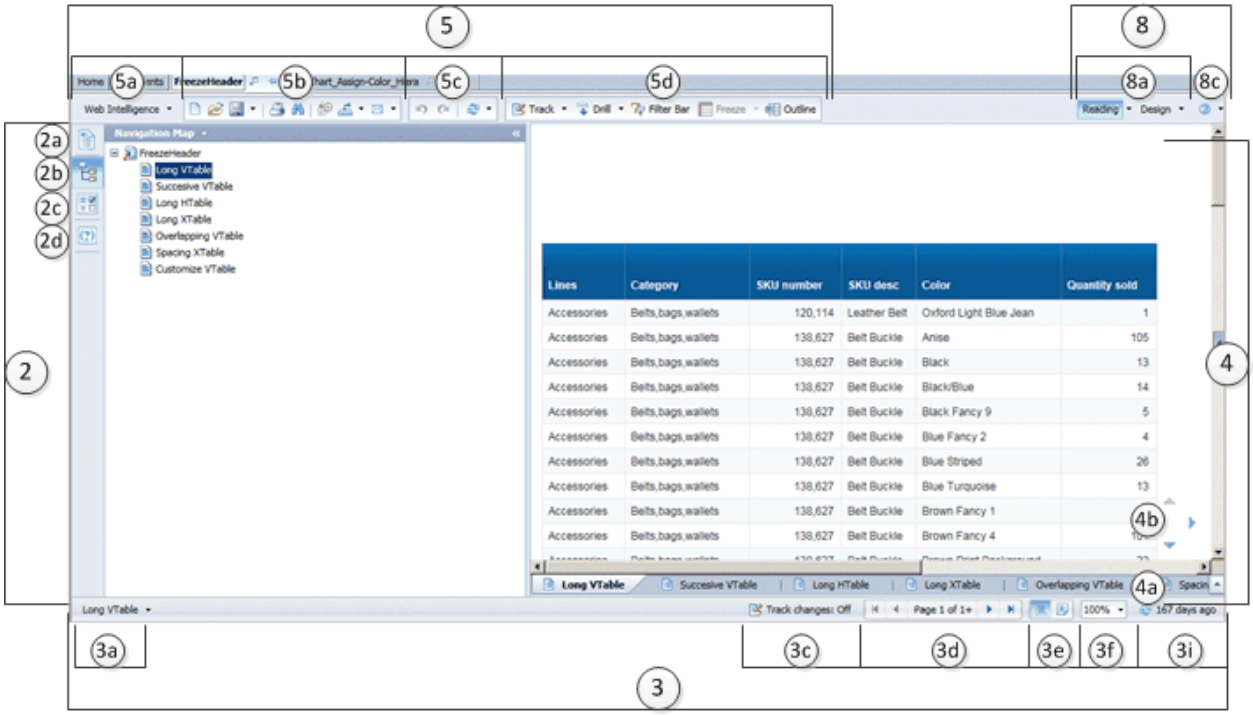


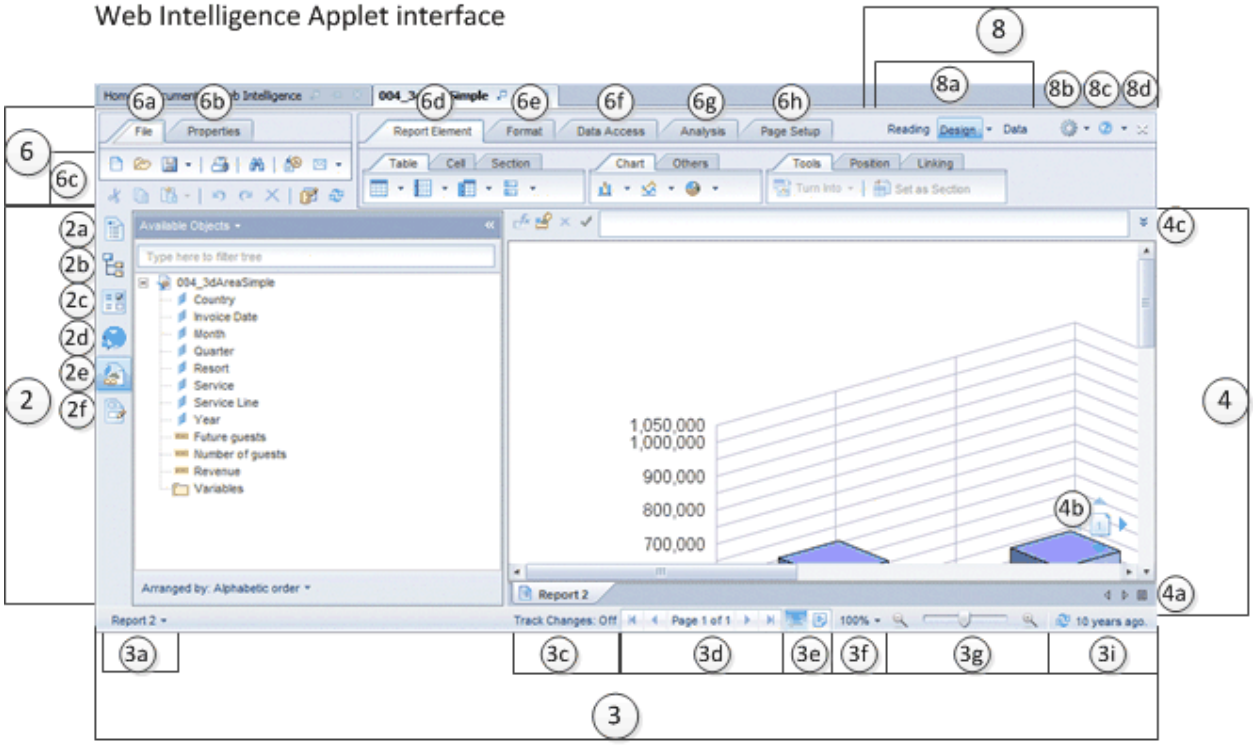
Figure 16: Reading Mode (English example)

Design Mode

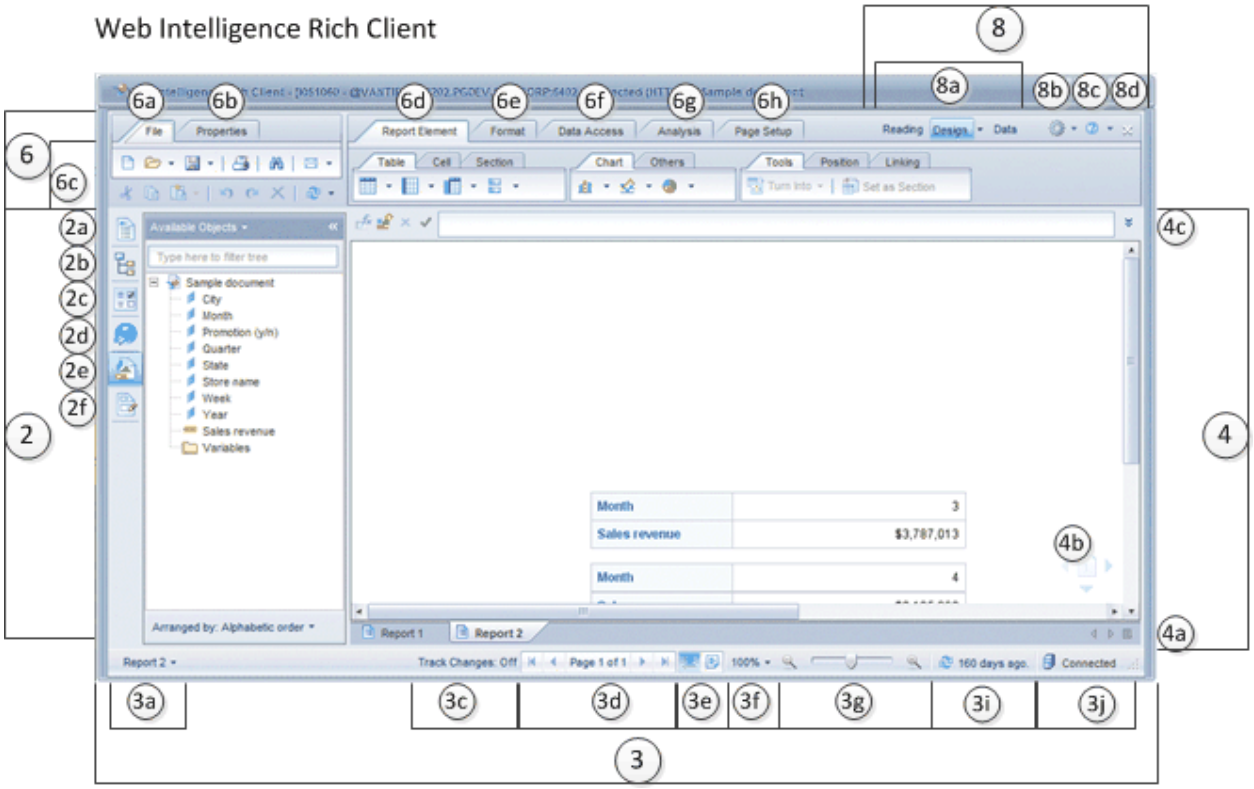
The following diagrams show the items that can be hidden in the Web Intelligence Design mode.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Web Intelligence Applet interface



Web Intelligence Rich Client



© 2015 SAP SE or an SAP affiliate company. All rights reserved.

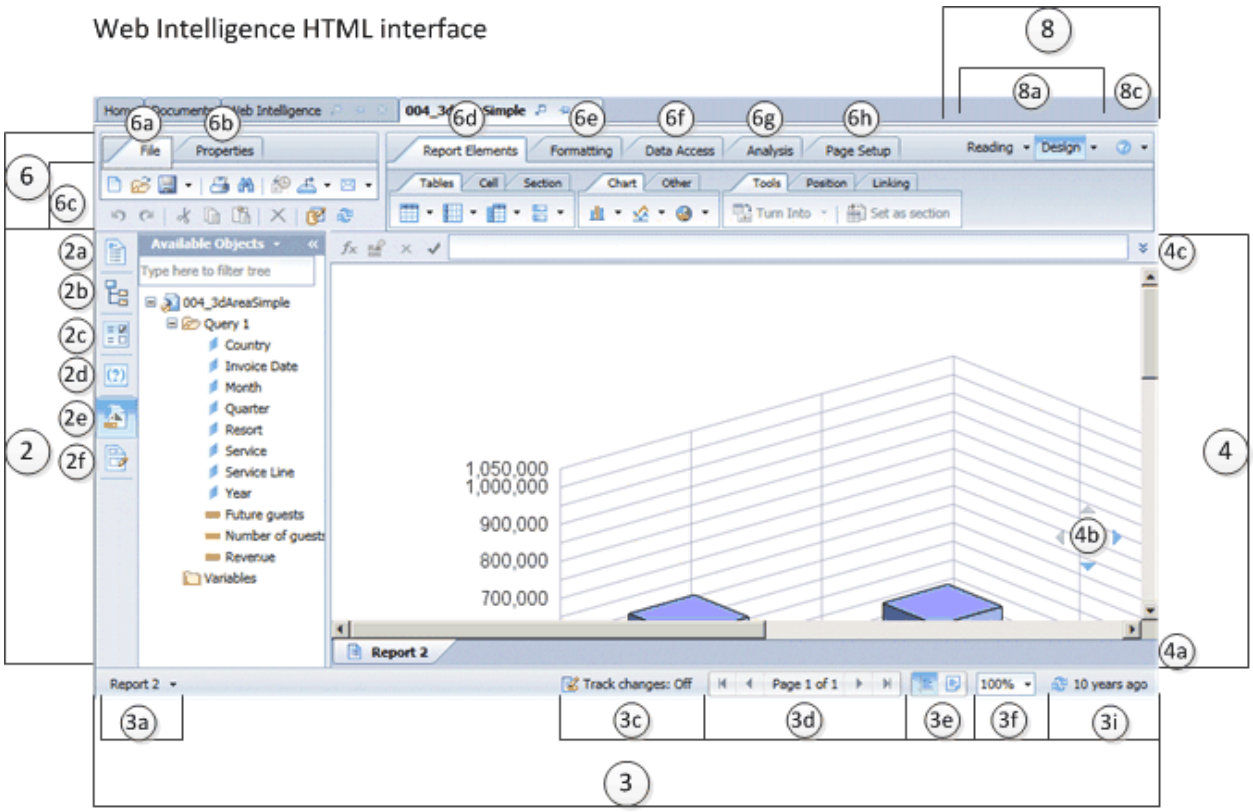


Figure 17: Design Mode (English example)

Data Mode

The following diagrams show the items that can be hidden in the Web Intelligence Data mode.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

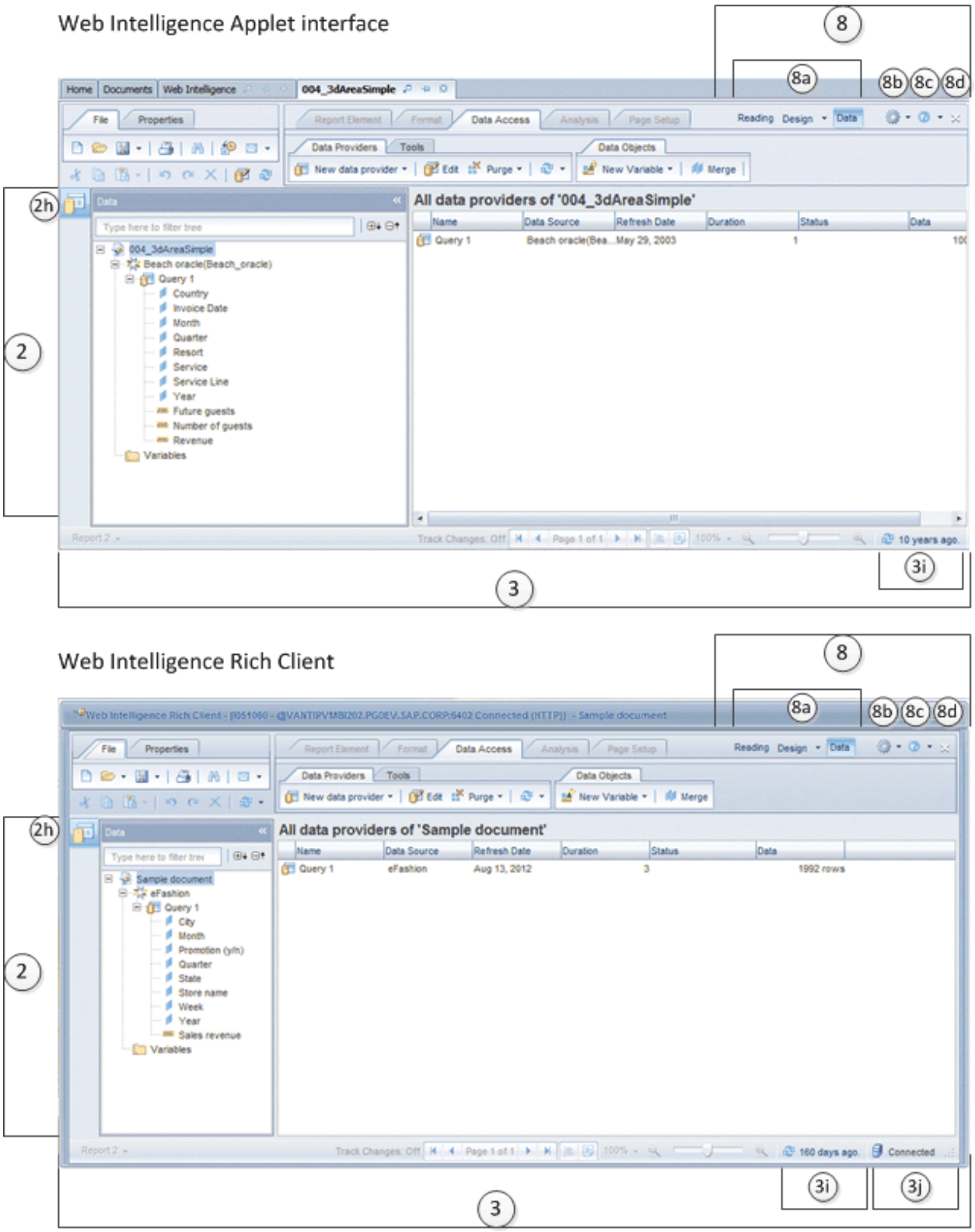


Figure 18: Data Mode (English example)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.4.1.1.2 Features tab

Table 88:

Feature Item	Description	Affects the following interface items
Refresh	Users can refresh documents to update the data from the data source.	The Refresh button in the Standard Action Group toolbar used in the Reading and Design modes.
Drill	Users can drill up and down on data in a document.	The Drill button available in the following locations: • The Analysis Group toolbar in the Reading mode. • The Interact subtab under the Analysis tab in Design mode.
Reading Mode	Users can view a document in Reading mode.	The Reading button in the following locations: • Application Contextual Menu • Application Control Toolbar
Design Mode	Users can view a document in Design mode.	The Design button in the following locations: • Application Contextual Menu • Application Control Toolbar
Data Mode	Users can view a document in Data mode.	The Data button in the following locations: • Application Contextual Menu • Application Control Toolbar

18.4.1.1.3 To customize the Web Intelligence interface appearance

You can customize the appearance of the Web Intelligence user interface by hiding menu items, sub-items, and features for a selected User Group and document folder.

1. Log into the CMC as an Administrator.
2. From the *Organize* list, select *Users and Groups*.
3. In the *Group Hierarchy* list, select a user group.
4. In the *Actions* list, select *Customization*.
5. In the Customization folders section, click *Add Folder* to add the folder containing Web Intelligence documents for which you want to apply customization for the selected user group.
6. Do one of the following:
   - To have items hidden in Web Intelligence, deselect them in the User Interface Elements or Features tab.
   - To have hidden items appear in Web Intelligence, select them in the User Interface Elements or Features tab.
7. Click *Save & Close*.

When you save the customization, all users of the selected group will see these changes the next time they log on to BI launch pad and open Web Intelligence.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> We recommend that you log on to BI launch pad as a user from the group you have just customized, start Web Intelligence, and verify that the interface corresponds to your customization settings.

18.4.1.2 Enabling Web Intelligence User Interface Extension Points for specific user groups

You can configure Web Intelligence rights to allow selected user groups to access customized interface extensions. Refer to the *SAP BusinessObjects BI Developer's Guide for Web Intelligence and the BI Semantic Layer* for more information about extension bundles and the REST web services API calls that are available.

18.4.1.2.1 To enable Web Intelligence User Interface Extension Points

To use the Extensions feature, you must have created and deployed the appropriate extension bundles in your installation. Deploy one extension bundle for each extension feature (for example, Custom Button, or Save as HTML).

1. Log into the CMC as an Administrator.
2. From the *Organize* list, select *Users and Groups*.
3. In the *Group Hierarchy* list, select a user group.
4. In the *Actions* list, select *Customization*
5. In the Customization folders section, click *Add Folder* to add the folder containing Web Intelligence documents for which you want to enable extension points for the selected user group.
6. Click the *Extensions* tab and select the custom extensions that you want the users to use.
7. Click *Save & Close*.

The enabled extensions are available to the selected user group when opening a document located in the selected folder. The extension points are available to all Web Intelligence application clients: web, Java Applet, and Rich Client.

18.4.1.3 Web Intelligence content alignment

Choose the way document content will be aligned (left-to-right or right-to-left) when users create Web Intelligence documents.

For the Web Intelligence Applet interface, you can set the content alignment in the CMC. Choose from these options:

- *Right-to-Left only when both the Preferred viewing and Product locales are set to Right-to-Left languages* (the default option)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- *Right-to-Left or Left-to-Right depending on the user's Preferred viewing locale*
- *Always Right-to-Left*
- *Always Left-to-Right*

> **Note**
>
> The content alignment setting applies to all users.

For the Web Intelligence Rich Client interface, the content alignment is determined by the locales set in the BI launch pad preferences:

- The system uses right-to-left alignment only when both the Preferred Viewing Locale and Product Locale are set to right-to-left languages.
- In all other cases, the content alignment is left-to-right.

> **Note**
>
> For information about how to set locales, see the *Business Intelligence Launch Pad User Guide*.

> **Note**
>
> Content alignment applies only at document creation time, and does not affect existing documents.

18.4.1.3.1 To set content alignment for the Web Intelligence Applet interface

Set content alignment for the Web Intelligence Applet interface.

1. Log into the CMC as an Administrator.
2. From the *Manage* list, select *Applications*.
3. Select *Web Intelligence*.
4. Click *Manage* > *Properties*.
5. Scroll down to the *Content Alignment for New Documents* section and select the appropriate option.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

18.4.2 BI launch pad

18.4.2.1 To enable the Clear button for prompts in the Schedule dialog box

When scheduling a Web Intelligence document based on a BEx query that contains SAP BW prompts, BI launch pad users can clear a prompt value so that it will be obtained by the SAP BW data source variable when the document runs.

1. Perform one of the following actions in the **<InstallDir>****<WebAppServer>**\webapps\BOE\WEB-INF\config\custom folder:
   - If an AnalyticalReporting.properties file is located in the folder, open the file in a text editor.
   - If no AnalyticalReporting.properties file exists in the folder, create a file with that file name, and open it in a text editor.
2. Perform one of the following actions in the AnalyticalReporting.properties file:
   - If the file already existed, locate the bex.dynamic_variable.schedule property in the file, and ensure that its value is set to true.
   - If you created the AnalyticalReporting.properties file, add bex.dynamic_variable.schedule=true to the end of the file..
3. Save and close the file, and then restart the web application server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

19 Managing Connections and Universes

19.1 Managing connections

A connection is a named set of parameters that defines how one or more SAP BusinessObjects applications can access relational or OLAP databases. Connection details such as server name, database, username, and password, can be stored securely in the BI platform repository in the Connections folder.

Designers define universes based on connections. Users of query, analysis, and reporting applications access the database via the universe without needing to know about the underlying data structures in the database.

You can create connections using the following applications:

- The universe design tool. Connections are stored in the repository.
- The information design tool. Connections can be created locally and then published to the repository, or created and edited directly in the repository.

> **Note**
>
> For information on how to manage OLAP data source connections, see the *SAP BusinessObjects Analysis, edition for OLAP Administrator Guide*.

You grant rights to allow users to create, edit, and delete connections.

You grant user access to universe connections and allow users to create and view documents that use universes and connections.

Related Information

Managing security settings for objects in the CMC [page 120]
Connection rights [page 852]

19.1.1 To delete a universe connection

> **Tip**
>
> It is also possible to delete connections in the universe design tool and the information design tool.

1. In the *Connections* area, select a universe connection from the list.
2. Click *Manage* > *Delete*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

19.2 Managing universes

A universe is an organized collection of metadata objects that enables business users to analyze and report on corporate data in non-technical language. These objects include dimensions, measures, hierarchies, attributes, pre-defined calculations, functions, and queries. The metadata object layer is built on a relational database schema or an OLAP cube, so the objects map directly to the database structures. A universe includes connections to the data sources so that users of query and analysis tools can connect to a universe and run queries and create reports using the objects in a universe without needing to know about the underlying data structures in the database.

You can create universes with the following tools:

- The universe design tool. Universes created with this tool can be distinguished by the .unv extension and are therefore called .unv universes. The .unv universes are defined on a secured connection and stored in the repository Universes folder.
- The information design tool. Universes created with this tool are based on the new semantic layer. They are distinguished by the .unx extension and are therefore called .unx universes. The .unx universes are authored locally and published to the repository Universes folder. Designers can define object-level security using the information design tool security editor.

You grant users application rights and universe rights to allow them to create, edit, and delete universes, as well as design security on universes.

You grant users universe rights to allow them to create and view documents that use universes.

Related Information

Managing security settings for objects in the CMC [page 120]
Universe design tool [page 861]
Universe (.unv) rights [page 848]
Information design tool [page 861]
Universe (.unx) rights [page 849]

19.2.1 To delete universes

> **Tip**
>
> It is also possible to delete universes in the information design tool.

1. In the *Universes* area of the CMC, select a universe in the list.
2. Click *Manage* > *Delete*.
3. When prompted for confirmation, click *OK*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

20 Monitoring

20.1 About Monitoring

The Monitoring application allows you to capture the runtime and historical metrics of BI platform servers, for reporting and notification. The monitoring application helps system administrators to identify 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 the BI platform.

Monitoring allows you to perform these tasks:

- Check the performance of each server: This is possible with the help of watches, which show the state of each server as traffic lights. The system administrator can set thresholds for these watches and receive alerts when these thresholds are breached. 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.
- View the entire BI platform deployment based on Server Groups, Service Categories, and Enterprise Nodes, both in graphical and tabular format.
- View the recent failures on the dashboard screen.
- Check system availability and response time: Using probes, you can simulate workflows to check if the servers and services in the BI platform deployment are functioning as expected. By analyzing the round-trip time of these probes at periodic intervals, the system administrator can assess the system usage pattern.
- Analyze peak load and peak period for the CMS: This helps the system administrator determine if more licenses or system resources are required.
- Integrate with other enterprise applications: The BI platform monitoring application can be integrated with other enterprise applications like SAP Solution Manager and IBM Tivoli Monitoring.

For more information about using the monitoring application, including details about probes and watches, see the *SAP BusinessObjects Business Intelligence platform CMC Online Help*.

Related Information

About the Server Metrics Appendix [page 902]

20.2 Monitoring terms

The following list provides terms that relate to the monitoring application:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Trend

To record or display historical data for the purpose of finding trends.

Dashboard

The Dashboard page provides a centralized view for the system administrator to monitor the performance of all servers. It provides real-time information on the system KPIs, recent alerts, and watches, and corresponding graphs based on the watch states.

Watch

Watches provide real-time status and historical trends of servers and workflows within the BI platform environment. Users can associate thresholds and alerts with watches. You can create a watch using data from probes, servers, SAPOSCOL, or derived metrics.

Derived metric

Derived metrics are metrics that you create by combining two or more existing metrics in a mathematical equation. You can create a metric based on the user's requirements, and then create a watch using this metric.

Topological metric

Topological metrics provide you with the net state for each service category in the BI platform. For example, the Crystal Reports service gives you the combined health state of all the watches related to Crystal Reports servers.

Health State

These are the health state values:

- "0" - "DANGER"
- "1" - "AMBER"
- "2" - "GREEN"

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

KPI

KPIs (key performance indicators) are standard metrics in the BI platform. They provide information about schedules and login sessions. For example, a higher number of *RunningJobs* indicates good performance of the servers. Alternatively, a higher number of *PendingJobs* indicates poor performance and high system load.

Probe

Probes monitor different services and simulate the different functionalities of the BI platform components. By scheduling probes to run at specified intervals, the system administrator can track the availability and performance of key services provided by the BI platform. This data can also be used for capacity planning.

Traffic light

A traffic light is an icon that displays the color Green, Amber, or Red to indicate the state of a watch at any given time. Users can choose to set two or three states to a watch.

Trending graph

A trending graph is a graphical representation of historical metric data generated by probes and servers. It helps the system administrator monitor the system at different time intervals, and assess the system usage pattern.

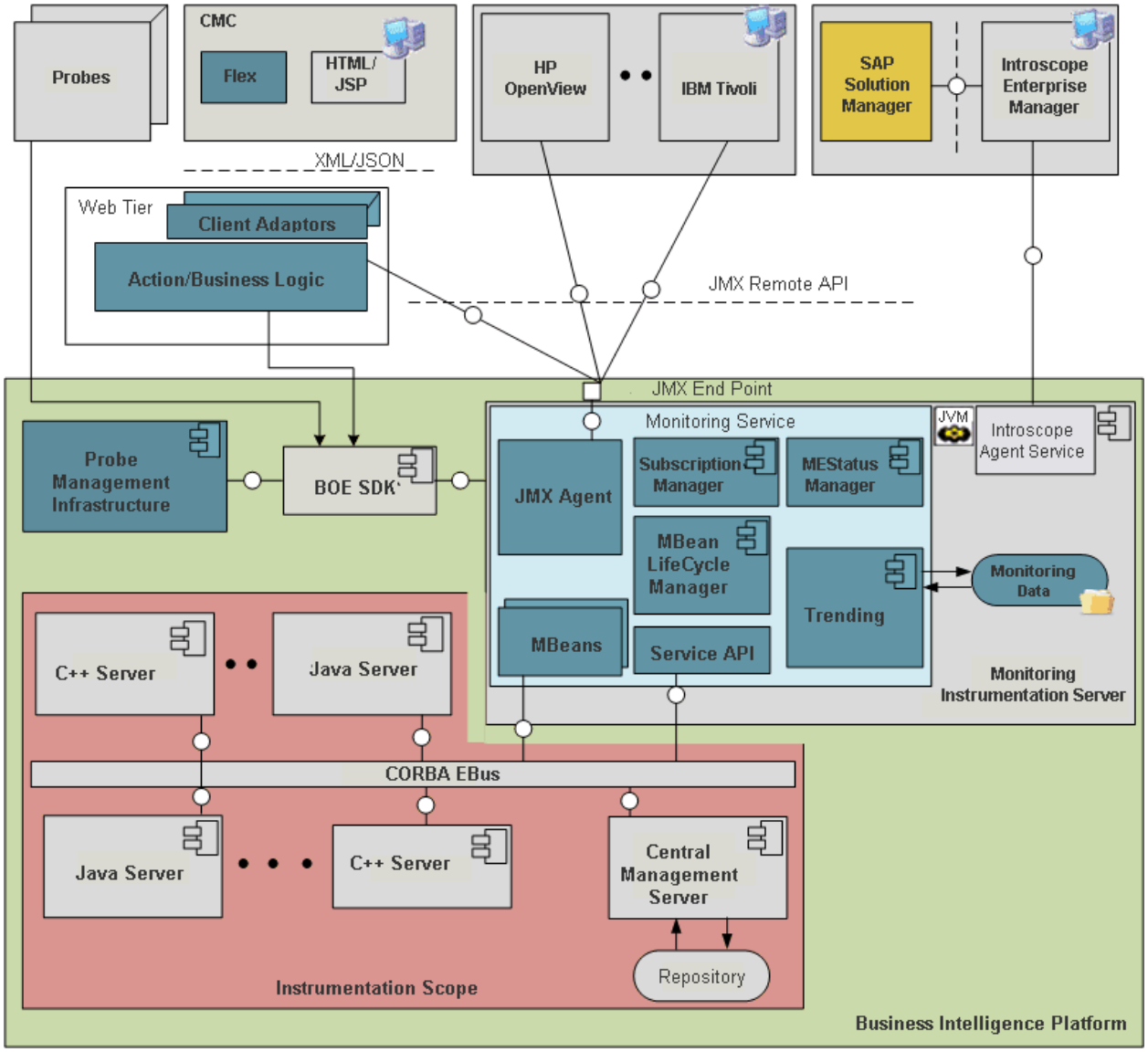
Alert

An alert is a notification generated by the monitoring application, when a user-defined threshold value set for different metrics applied to a watch is breached. You can choose to receive alerts either through email or on the *Dashboard* page.

20.2.1 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:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.



The high-level components in the architecture are listed below:

- The Adaptive Processing Server (APS)
- The Java Management Extensions (JMX) agent/server
- MBeans
- JMX Clients
- The Management consoles
- Trending Database

The monitoring service is hosted on the Adaptive Processing Server. The application is based on JMX technology.

The Monitoring Service provides the core services available in the monitoring application. The Monitoring Service provides the following services:

- Provides the JMX agent service.
- Creates MBeans dynamically for the SAP BusinessObjects servers.
- Provides lifecycle management for the MBeans.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Provides a mechanism for registering new probes.
- Allows users to create complex threshold conditions using the metrics of the servers.
- Provides a threshold notification mechanism and sends alerts.
- Stores historical data.

The Probe Scheduling Service that is hosted on the Adaptive Job Server manages the running and scheduling of probes. Hence, the Adaptive Job Server should be running for the probes to run.

The monitoring application also exposes a JMX or Remote Method Invocation (RMI) URL end point. Other enterprise applications such as IBM Tivoli Monitoring can connect to the monitoring application and access the BI platform metrics by using a JMX Remote API. The monitoring application uses a dedicated Derby database for storing historical data for the purpose of trending. For information on the trending database schema, see Trending database schema [page 937].

20.3 Configuring database support for Monitoring

This section describes how to set up monitoring, and report against monitoring data.

> **Note**
>
> Only watches that have the setting *Write to Trending Database* selected write monitoring information to the trending database.

There are two database options for recording monitoring information:

- Record information in the embedded Derby database (the default option).
  The monitoring application includes an embedded Apache Derby database, often referred to as the “trending database”, where monitoring information is stored by default. Users can report from the Derby database; however, it does not provide failover or traditional relational database backup and recovery tools. Also, the Derby database must be manually refreshed to return the latest information.
- Record information to the auditing database (the relational database where the CMS stores auditing data).
  Instead of using the default Derby database, you can choose to use the Auditing Data Store (ADS), often referred to as the auditing database. You can use either the auditing database included with the BI platform, or another supported database that you've configured as your auditing database. Using the auditing database allows users to report from the auditing data together with the monitoring information. Capturing the data in a relational database provides backup and recovery capability, and the real-time availability of data.

Related Information

Configuration for using the Derby database [page 612]
Configuration for using the auditing database [page 612]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

20.3.1 Configuration for using the Derby database

The monitoring application stores monitoring data in the embedded Derby database by default. If you want to use the Derby database, confirm the following database setting in the CMC:

1. In the *Manage* area on the CMC home page, click *Applications*.
2. Double-click *Monitoring Application* to open the properties page.
3. In the *Trending Database Settings* area, verify that *Use Embedded Database* is selected.

To run queries in the Derby database to create reports and perform data analysis, a universe is required for the Derby database. A universe is provided with your BI platform deployment, at this location in the CMC: *Universes* > *Monitoring TrendData Universes*.

20.3.2 Configuration for using the auditing database

If you want to use the auditing database for your monitoring data, you will need to perform extra configuration steps as follows:

- If you have existing data in your Derby trending database, you will need to migrate the Derby database to the auditing database, and then configure the BI platform to record monitoring information in the auditing database. These are the high-level steps you'll need to follow. For details, see the related topics.
  1. Migrate the Derby database.
  2. Configure the SBO files and add alias names.
  3. Switch to the auditing database.
  4. Restart the Adaptive Processing Server that hosts the Monitoring Service.
  5. On the Monitoring Dashboard, ensure that everything works as expected. Verify that these monitoring tables have been created in the database:

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- If you do not have data in your trending database, that is, you have a fresh installation, you do not need to migrate the database; you only need to configure the BI platform to record monitoring information in the auditing database. These are the high-level steps you'll need to follow. For details, see the related topics.
  1. Verify that the auditing database is working, and auditing is running properly.
  2. Create the monitoring tables in the ADS.
  3. Configure the SBO files and add alias names.
  4. Switch to the auditing database.
  5. Restart the Adaptive Processing Server that hosts the Monitoring Service.
  6. On the Monitoring Dashboard, ensure that everything works as expected. Verify that these monitoring tables have been created in the database:

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

MOT_TREND_DETAILS

> **Note**
>
> If you record Monitoring data to the auditing database, and you want to report from this data, you will need to develop a custom universe. The universe included with the BI platform is for use with the embedded Derby database only.

Related Information

Migrating the Derby database to the auditing database [page 613]
Configuring SBO files [page 615]
Adding alias names in the SBO file [page 617]
To switch to the auditing database [page 618]
To create the monitoring tables in the ADS [page 614]

20.3.2.1 Migrating the Derby database to the auditing database

If you want to use the auditing database for your monitoring data, and you have existing data in your Derby trending database, you will need to migrate the Derby database to the auditing database.

Before you start migrating your data, verify these prerequisites:

- The auditing database is working, and auditing is running properly.
- You have sufficient authorizations and database client applications on the target database to create new tables, import CSV dumps, and so on.
- The auditing database supports the import of comma-separated values (CSV) files.

Follow these steps to perform the database migration:

1. To back up the Derby database [page 614]
2. To export the data into CSV files [page 614]
3. To create the monitoring tables in the ADS [page 614]
4. To restore contents to the target database [page 615]

> **Note**
>
> In a clustered scenario, users are expected to use the same instance of the Derby database for all the Monitoring instances. If the user has more than one Derby database instance in a clustered scenario, the user should only import the data from one Derby instance. Importing data from multiple Derby instances will result in data inconsistency and is therefore not recommended.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

20.3.2.1.1 To back up the Derby database

1. In the *Manage* area on the CMC home page, click *Applications*.
2. Double-click *Monitoring Application* to open the properties page.
3. In the *Trending Database Settings* area, enter a file location to back up the Derby trending database to, and click *Save*.
4. Beside *Run database backup task*, click *Now*.

   A confirmation message appears if the database backup is successful. Also check the folder location you entered for the backup location, and verify that the backup files have been placed there.

20.3.2.1.2 To export the data into CSV files

This section explains how to generate the CSV dump files required for migration. The CSV files contain comma-separated values of the embedded Derby database data content.

1. In the *Manage* area on the CMC home page, click *Applications*.
2. Double-click *Monitoring Application* to open the properties page.
3. In the *Trending Database Settings* area, beside *Export Data from Embedded database as CSV files*, click *Export*.

The following four CSV files are generated in the default Trending Database location, which is `<BOE_Install_Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB`:

- Mot_Mes_Details.csv
- Mot_Trend_Data.csv
- Mot_Trend_Details.csv
- Mot_Mes_Metrics.csv

20.3.2.1.3 To create the monitoring tables in the ADS

Follow these steps to prepare the target auditing database:

1. After installing the BI platform, DDLs related to all the supported CMS auditing databases are available in the `<Install Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` location. You will find seven different (.sql extension) files with the respective database name. For example: `Oracle.sql` for Oracle, `Sybase ASE.sql` for Sybase ASE Database, and so on.
2. Go to the target database (in this case, the target database is the database where CMS auditing has been configured) and run the .sql file. The following four Monitoring tables are created: `MOT_TREND_DETAILS`, `MOT_TREND_DATA`, `MOT_MES_DETAILS`, and `MOT_MES_METRICS`. The required indexes are also created, along with the tables.

If all the tables are created with correct data types as mentioned in the .sql file, the database schema required for the Monitoring application is created.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

20.3.2.1.4 To restore contents to the target database

The following steps need to be performed in order to restore the content to the target database:

1. Enable Identity Insert.

   The Monitoring tables contain a number of IDENTITY columns. These are columns that auto-generate their values. Certain databases (for example MS SQL Server and Sybase ASE) do not allow explicit insertion of values to these columns. During data migration, even these identity column values need to be migrated however. Users therefore have to enable the explicit insertion of these values using the following SQL command: `SET IDENTITY_INSERT <TABLE NAME> ON`.

2. Import the CSV dump file to the target table.

   All software provided by database clients enables users to import the data from CSV to the table using either a menu option or a command. The user needs to use this option to import the data from the CSV file to the corresponding table. Import the data files into the new tables in the following order:

   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `MOT_MES_METRICS`

3. Disable Identity Insert.

   Once the data has been imported, the user needs to disable the identity insert on the table using the following SQL command: `SET IDENTITY_INSERT <TABLE NAME> OFF`.

   Users have to disable the identity insert on a table after the data import in order to enable the identity insert on the next table. This is because the identity insert operation can be enabled on only one table at a time.

Enabling or disabling Identity Insert applies only to MS SQL Server and Sybase ASE. For other databases such as Oracle, MaxDb, DB2, MySQL, or SQL Anywhere, this is not required. You can import the data to the tables directly.

20.3.2.2 Configuring SBO files

Internally, the Monitoring application uses Connection Server libraries, and the SBO configuration is required for the Connection Server to establish connectivity to the database driver. You need to specify the database driver and its location in the SBO file to establish this connectivity.

> **Note**
>
> The Monitoring application refers to the auditing connection name, and uses JDBC if `<hostName>.<Portnum>.<dbName>` is used, or ODBC otherwise. The Connection Server SBO files need to be configured accordingly for the Monitoring application to be able to connect to the auditing database.

> **Note**
>
> For Oracle databases, only JDBC connections are supported.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Example

- If the Connection name field configured in the CMC Auditing page is `<hostName>.<Portnum>.<dbName>`, the driver JAR should be configured in: `dataAccess\connectionServer\jdbc\<dbType>.sbo`.
- If the Connection name field configured in the CMC Auditing page is an ODBC DSN, the driver should be configured in: `<Install_Dir>\dataAccess\connectionServer\odbc\<dbType>.sbo`.
- If the database used for auditing is SAP HANA, the file where the driver needs to be configured is: `<Install_Dir>\dataAccess\connectionServer\odbc\newdb.sbo`.
- If the database used for auditing is MS SQL Server, the file where the driver needs to be configured is: `<Install_Dir>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- If the database used for auditing is DB2 server, the connection server does not contain a supporting `db2iseries.sbo` file.
  By default, the monitoring application uses the ODBC connection mode to connect to the DB2 auditing database. To work in this mode, you must add and configure the System DSN (for the DB2 server) in the machine on which monitoring application is running. For information on how to add and configure the ODBC connection for DB2, refer the following links:
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024166.htm
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024200.htm

Note

If you do not configure the System DSN for DB2, the monitoring trending fails.

Configuring SBO files

Typically, the ODBC libraries are already configured in the SBO files and you just need to add the alias names. If this is not the case, follow these examples to perform the configuration in the SBO file:

Example

- If the database version used for auditing is SAP HANA, the configuration in SBO should be:

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
    <Aliases>
        <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
        <Alias>Hana</Alias>
    </Aliases>
    <Libraries>
        <Library Platform="MSWindows">dbd_wnewdb</Library>
        <Library Platform="MSWindows">dbd_newdb</Library>
    </Libraries>
    <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- If the database version used for auditing is MS SQL Server 2008, the configuration in SBO should be:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
    <Libraries>
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
        <Library>dbd_wmssql</Library>
        <Library>dbd_mssql</Library>
    </Libraries>
    <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
    <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
    <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
    <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- id="li_9D4EB94F9752458BB21A940C0A892C6D">If the database version used for auditing is MySQL 5, the SBO should have this entry:

```
<DataBase Active="Yes" Name="MySQL 5">
    <JDBCDriver>
        <ClassPath>
            <Path>C:\mysqljdbcdriver.jar</Path>
              </ClassPath>
        <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
        <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</
Parameter>
    </JDBCDriver>
    <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
    <Parameter Name="Force Execute">Always</Parameter>
    <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

- If the database version used for auditing is Oracle, the configuration in SBO should be:

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>
               <Path>C:\app\Administrator\product\11.2.0\client_64\jdbc\lib
\ojdbc6.jar</Path>
             </ClassPath>
                <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
                <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
       </JDBCDriver>
       <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
        <Parameter Name="Escape Character">/</Parameter>
         <Parameter Name="Force Execute">Always</Parameter>
         <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

For more information on configuring the driver in SBO files, refer to the *Data Access Guide*.

20.3.2.3 Adding alias names in the SBO file

In addition to configuring the driver, users also need to add an alias in the SBO, under the database version that is being used for auditing. The following table lists the alias names that should be used for specified databases.

DB Name	Alias Name to be used in SBO
SAP HANA	Hana

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

DB Name	Alias Name to be used in SBO
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

You need to use the specified names, as the Monitoring application searches the SBO for these names.

Example

If the database used for auditing is MS SQL Server 2008, the alias needs to be added to the SBO as shown:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
   </DataBase>
```

20.3.2.4 To switch to the auditing database

Switch the database so that Monitoring trending information will be stored in the auditing database.

1. In the *Manage* area on the CMC home page, click *Applications*.
2. Double-click *Monitoring Application* to open the properties page.
3. In the *Trending Database Settings* area, select *Use Audit Database*.

Note

If you are using an Oracle database for auditing, the *ADS Database Connection Name* on the Auditing page in the CMC needs to be specified as a JDBC connection. Specify the connection name as follows: **<server_name>,<port>,<service_name>**.

Note

To ensure that the monitoring tables are created correctly, grant the following permissions for the database user account:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

EXECUTE
CREATE SEQUENCE
CREATE TRIGGER

20.4 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* tab of the CMC.
2. Right-click *Monitoring Application* and select *Properties*. The *Monitoring Application Properties* window appears. The configurable properties are described in the following table:

Table 89:

Section	Field	Description
	Enable Monitoring Application	Select this option to enable monitoring functionality. If you deselect this option, all monitoring functions except probes will be disabled. Probe trending will also be disabled.
	Default JMX agent end point URL (IIOP)	This contains the default JMX agent end point URL that uses the IIOP protocol. This URL is generated automatically if you enable monitoring and then restart the server. This is the default protocol for the monitoring service. This is a read-only field.
RMI	*Enable RMI protocol for JMX*	By default, this option is disabled. If you enable this option, you must provide the RMI port number. This port will be used for both RMI registry entry and RMI connector port. This port should be available for the service; otherwise the service will fail to start. After you provide the RMI port number, restart the server. Once the server is restarted, the RMI JMX agent end point URL is generated. This is a read-only property containing the JMX agent's end point URL using the RMI protocol. Use this URL to connect to monitoring from other clients.
Host Metrics	*Enable host metrics*	By default, this option is disabled. If you enable this option, you must provide the path to your installation of the SAPOSCOL binary To enable host metrics, you need to install SAPOSCOL. For more information on how to install SAPOSCOL, see “Installing SAPOSCOL”.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Section	Field	Description
Trending Database Settings	*Use Audit Database*	Select this option to store the trend history of metrics in the CMS auditing database. **Note** CMS Auditing has to be configured for this to work.
	Use Embedded Database	Select this option to store the metric/watch trend history in the embedded database, which comes with the Monitoring application.
	Delete older data when the database size grows more than (MB)	Data from the trending database will be cleaned up when the database exceeds the specified size. A 30% buffer is created for the database. For example, if you have set this property to 100 MB, and if the database has grown larger than 100 MB when the system checks, data will be cleared until the database is 70 MB.
	Run database cleanup task everyday at	The database cleanup task starts at the time specified. The database will be cleaned when the database exceeds the specified maximum size.
	Backup trending database every	Specifies the number of hours between each backup of the trending database. If this value is set, a backup will occur when the system starts, or whenever the APS is restarted, and also at every interval specified.
	Trending database backup directory	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.
	Run database backup task	The database backup task starts when you click this option. Specify the database backup directory location before choosing this option.
	Export Data from Embedded database as CSV files	Click the *Export* button to export the database as comma-separated-value files.
	Trending database location	By default, the trending database location is **<INSTALLDIR>**`\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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Section	Field	Description
Other settings	*Metric Refresh Interval (seconds)*	The minimum interval that you can specify is 15 seconds. This interval governs the following: ○ Subscription computation of the watches: The caution and danger rules are computed continuously with the specified time interval. ○ Calculating the watch state: Watch states are computed continuously with the specified time interval if the Event setting of the watch is selected with the following option: *Change the watch state every time caution or danger evaluates to true*. ○ Trending period: History mode for the graphs is recorded continuously with the specified time interval.
	Monitoring UI auto refresh interval (seconds)	This interval will be used in the monitoring user interface (including the dashboard, watch list, and probes) for auto refresh. The minimum interval is 15 seconds. Auto-refresh does not affect the time duration in Live mode in graphs, which is set to 15 seconds by default.
	Alert Reminder Frequency (days)	Specifies the number of days before an alert reminder is generated.

3. Click *Save*.

> **Note**
>
> When you change any of these properties except enabling and disabling the monitoring application, you must restart the Adaptive Processing Servers that host the monitoring services.

Installing SAPOSCOL

Perform the following steps to install SAPOSCOL:

1. Download `SAPHOSTAGENT710_XX.SAR` from SAP Marketplace (http://service.sap.com).
2. Extract `SAPHOSTAGENT710_XX.SAR` by executing the `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR` command.
3. Install `saphostexec` by executing the `saphostexec.exe -install` command. Once saphostexec is installed as a service, SAPOSCOL is started.
4. Check SAPOSCOL status by executing the `saposcol -s` command.

20.4.1 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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

(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 [page 619].

20.4.2 HTTPS authentication for monitoring probes

HTTPS server authentication for monitoring probes is supported, and requires the following configuration prior to use:

1. Import the server certificate into the client's truststore. This allows the client side (the probe) to verify the server's identity. Run this command: `<INSTALL_ROOT>\SAP BusinessObjects Enterprise XI`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore "<INSTALL_ROOT>\SAP
BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" -file
ca.cer
```

`ca.cer` is either the server's self-signed certificate, or the certificate of the Certificate Authority (usually an internal CA) that generated the server's certificate. If the server's certificate is generated by a well known CA, then there is no need to import it, and this step can be skipped. This is because the server's certificate will be verified with the CA, whose public key is already in the truststore by default.

2. Change the *URL base* in the BI launch pad probe's settings to `https://<URL>/BOE/BI`, where <URL> refers to the host by the name used in the certificate.

HTTPS client authentication for monitoring probes is not supported.

20.4.3 Password encryption for probes

When using probes, to ensure that passwords are encrypted, you must add the `true` parameter to every monitoring probe's password parameter when you create the probe through the command line. For more information and a syntax example, see the topic *Managing Probes Through the Command Line* in the CMC help.

20.5 Integrating with other applications

Enterprise solutions, such as IBM Tivoli Monitoring, integrate with the monitoring application as JMX clients connecting via the JMX end point URL. After integration, the SAP BusinessObjects metrics can be viewed from the client's user interface.

20.5.1 Integrating the monitoring application with IBM Tivoli

To integrate the 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 the BI platform
Password	The password that is used to log into the BI platform
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 the 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 from 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 the BI platform using the Agent Builder, then you need to have the BI platform 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 BI platform monitoring installed because at configuration time you can provide 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 the 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 the 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 the **<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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Configuration properties [page 619]

20.5.2 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 BI platform 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 the BI platform 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 CMC help.
>
> For the JMX metrics to be available in IS, ensure that both the IS agent services and monitoring service are available on the AdaptiveProcessingServer Instance.
>
> If you enable IS instrumentation, the code instrumentation is enabled automatically.

20.6 Cluster support for monitoring server

The monitoring application supports clustering, which provides failover capability.

With cluster support, only one service is active at any given time, and all other services are passive. If there are two monitoring services s1 and s2 in a clustered environment, only one of them is available. Both s1 and s2 attempt to become active, but when one of them succeeds, the other service becomes inactive or passive.

The passive service checks the availability of the active service periodically (every minute). If the active service is unavailable, the passive service immediately attempts to become active.

> **Note**
>
> It is recommended that the monitoring service be hosted on a separate Adaptive Processing Server (APS) instance to avoid failures or poor performance of the APS.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

20.7 Troubleshooting

This section provides step-by-step solutions to a wide range of problems that may occur in your work with the monitoring application.

20.7.1 Dashboard

Monitoring link is not displayed on the CMC page

- Check if the user has adequate access rights.
- Ensure that the user is added to the Monitoring User or Administrator groups or any other group which is a part of these groups.

Key Performance Indicators (KPIs) are not visible on the Monitoring Dashboard

- Check if the required metrics are visible by choosing *CMS Server properties* > *Metrics*.
- Ensure that the Central Management Server is responding as expected.

Unable to launch the monitoring application

Download and install the latest Flash player.

20.7.2 Alerts

Unable to receive alerts on the Alerts page

- Check if the *Enable My Alerts* option in the Alerting application properties is selected.
- Ensure that you have adequate access rights to receive alerts.
- Check if the recent alerts are visible on the monitoring dashboard.

> **Note**
>
> You can send a Crystal Reports document to the email ID you set to test if the SMTP is working as expected.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Unable to receive email notifications

- Check if the *Enable Email* option in the Alerting application properties is selected.
- Check if the email address settings for receiving email alerts is appropriate.
- Check if the SMTP server is functioning.
- Ensure that the Adaptive Job Server instance is enabled.
- Check the SMTP settings in the Adaptive Job Server instance destination.

20.7.3 Watchlist

Unable to receive historical data for Watch

- Check the polling interval on the monitoring application *Properties* page.
- Check the trace file in the logging folder.
- Check if the *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 Adaptive Processing Server instance is running.

Watchlist tab is disabled

- Check if the Monitoring service is running.
- Check the monitoring service logs for error messages.
- Check if the servers and their metrics are visible in jConsole.

Related Information

Configuration properties [page 619]

 © 2015 SAP SE or an SAP affiliate company. All rights reserved.

20.7.4 Probes

Unable to schedule Probes

- Check if the AdaptiveJobServer instance that hosts the Probe Scheduling Service is running.
- Ensure that the report CUID, that is used for Crystal Reports and Web Intelligence documents, is appropriate.
- Ensure that the user has administrative rights or is a member of the Administrator group.
- Check if the user has adequate rights to open, refresh, export Crystal Reports or Web Intelligence documents that are used in the corresponding probes.

Probe schedule status is pending

- Check if the ProbeSchedulingService instance is installed.
- Check if the AdaptiveJobServer instance that hosts the Probe Scheduling Service is running.

An error occurred while retrieving the trend data from the database

Check if the AdaptiveProcessingServer instance is running.

probeRun.bat fails to run successfully

- Check if `java_home` is set.
- Check if the correct parameters are entered in the command prompt.

> **Note**
>
> Enter **`probeRun.bat -help`** in the command prompt to check if all the parameters are appropriate.

20.7.5 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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

20.7.6 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

21 Auditing

21.1 Overview

Auditing allows you to keep a record of significant events on servers and applications, which helps give you a picture of what information is being accessed, how it's being accessed and changed, and who is performing these operations. This information is recorded in a database called the Auditing Data Store (ADS). Once the data is in the ADS, you can design custom reports to suit your needs. You can look for sample universes and reports on the SAP Community Network http://scn.sap.com/.

For the purposes of this chapter, an auditor is a system responsible for recording or storing information on an event, and an auditee is any system responsible for performing an auditable event. There are some circumstances where a single system can perform both functions.

How Auditing works

The Central Management Server (CMS) acts as the system auditor, while each server or application that triggers an auditable event acts as an auditee. When an audited event is triggered, the auditee will generate a record and store it in a local temporary file. At regular intervals, the CMS communicates with the auditees to request these records and writes the data to the ADS.

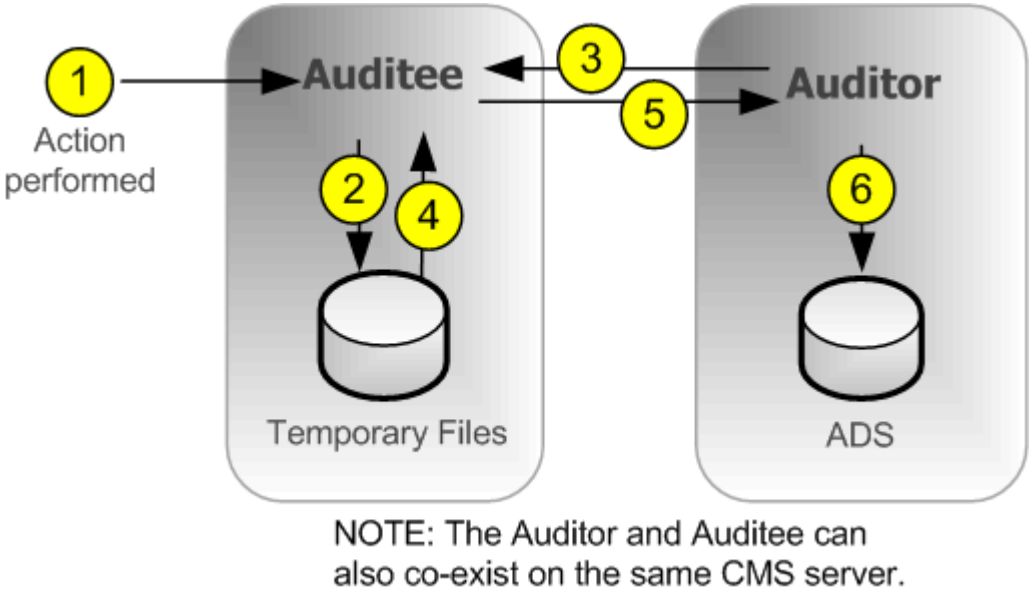
The CMS also controls the synchronization of auditing events that occur on different machines. Each auditee provides a timestamp for the auditing events that it records. To ensure that the timestamps of events on different servers are consistent, the CMS periodically broadcasts its system time to the auditees. The auditees then compare this time to their internal clocks. If differences exist, they correct the time recorded for subsequent auditing events.

Depending on the type of auditee, the system uses one of the following workflows to record the events.

Server auditing

In cases of server generated events, the CMS can act as both Auditee and Auditor.

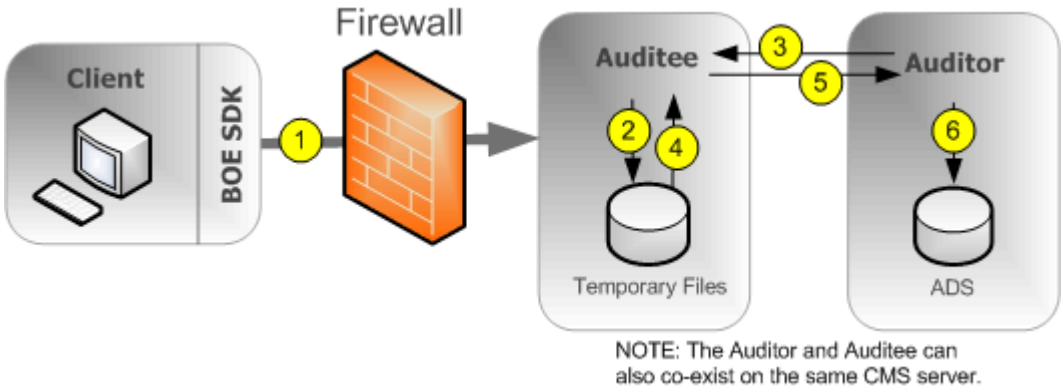
© 2015 SAP SE or an SAP affiliate company. All rights reserved.



1. An auditable event is performed by the server.
2. The auditee writes events in a temporary file. Steps 1 and 2 can occur multiple times before step 3.
3. At regular intervals, the auditor polls the auditee and requests a batch of auditing events.
4. The auditee retrieves the events from the temporary files.
5. The auditee transmits the events to the auditor.
6. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

Client logon auditing for clients connecting through CORBA

This includes applications such as SAP BusinessObjects Web Intelligence.



1. The client connects to the CMS, which will act as the auditee. The client provides its IP address and machine name, which the auditee then verifies.

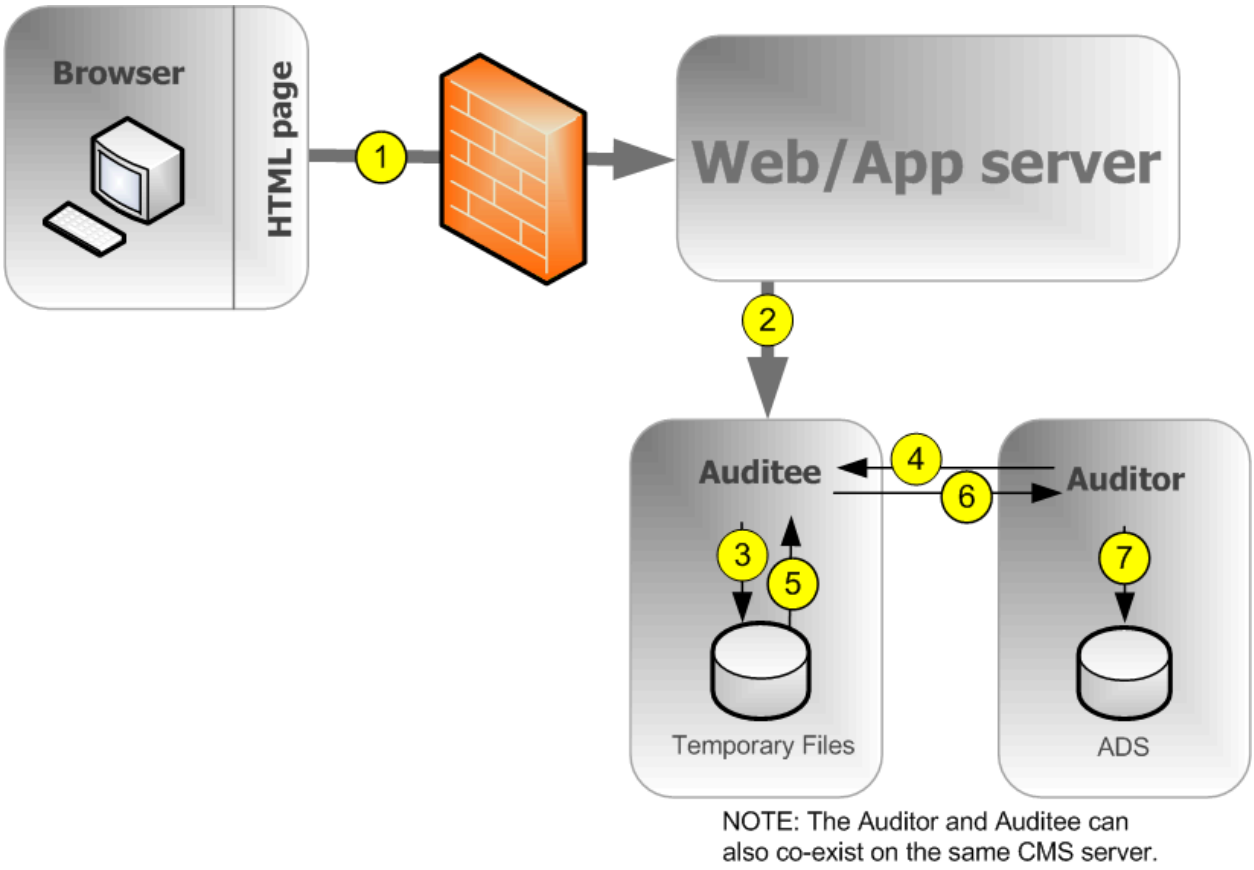
> **Note**
>
> A port should be opened in the firewall between the client and CMS. More details on firewalls can be found in the security chapter of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. The auditee writes events in a temporary file. Steps 1 and 2 can occur multiple times before step 3.
3. At regular intervals, the auditor polls the auditee and requests a batch of auditing events.
4. The auditee retrieves the events from the temporary files.
5. The auditee transmits the events to the auditor.
6. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

Client logon auditing for clients connecting through HTTP

This includes online applications such as BI launch pad, Central Management Console, SAP BusinessObjects Web Intelligence, and so on.

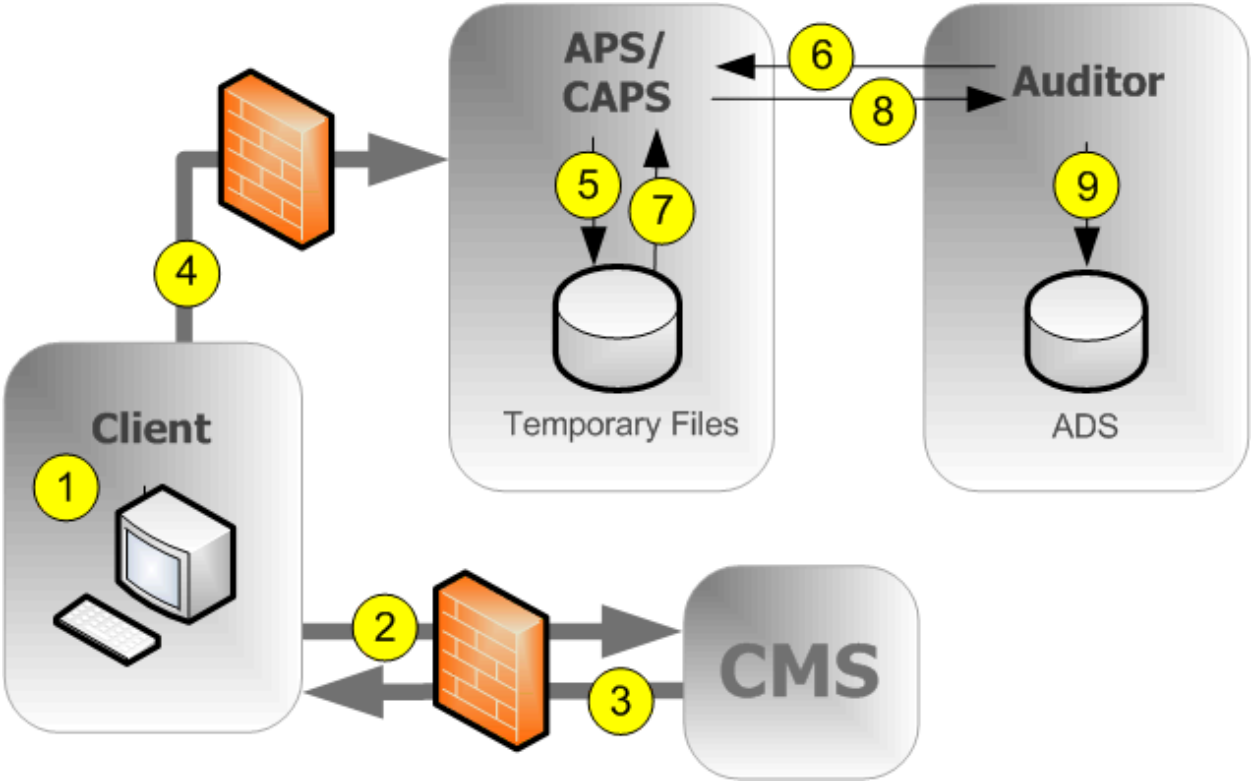


1. The browser connects to the web application server, and logon data is submitted to the web application server.
2. The BI platform SDK submits the logon request to the auditee (CMS), along with the IP address and name of the browser machine.
3. The auditee writes events in a temporary file. Steps 1 to 3 can occur multiple times before step 4.
4. At regular intervals, the auditor polls the auditee and requests a batch of auditing events.
5. The auditee retrieves the events from the temporary files.
6. The auditee sends events to the auditor.
7. The auditor writes events to the ADS and signals the auditee to delete the events from the temporary files.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Non-Logon auditing for clients connecting through CORBA

This workflow applies to auditing SAP BusinessObjects Web Intelligence events when connecting through CORBA.



1. The user performs an operation that may be audited.
2. The client contacts the CMS to check if the operation is configured to be audited.
3. If the action is set to be audited, the CMS communicates this information to the client.
4. The client sends the event information to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server.

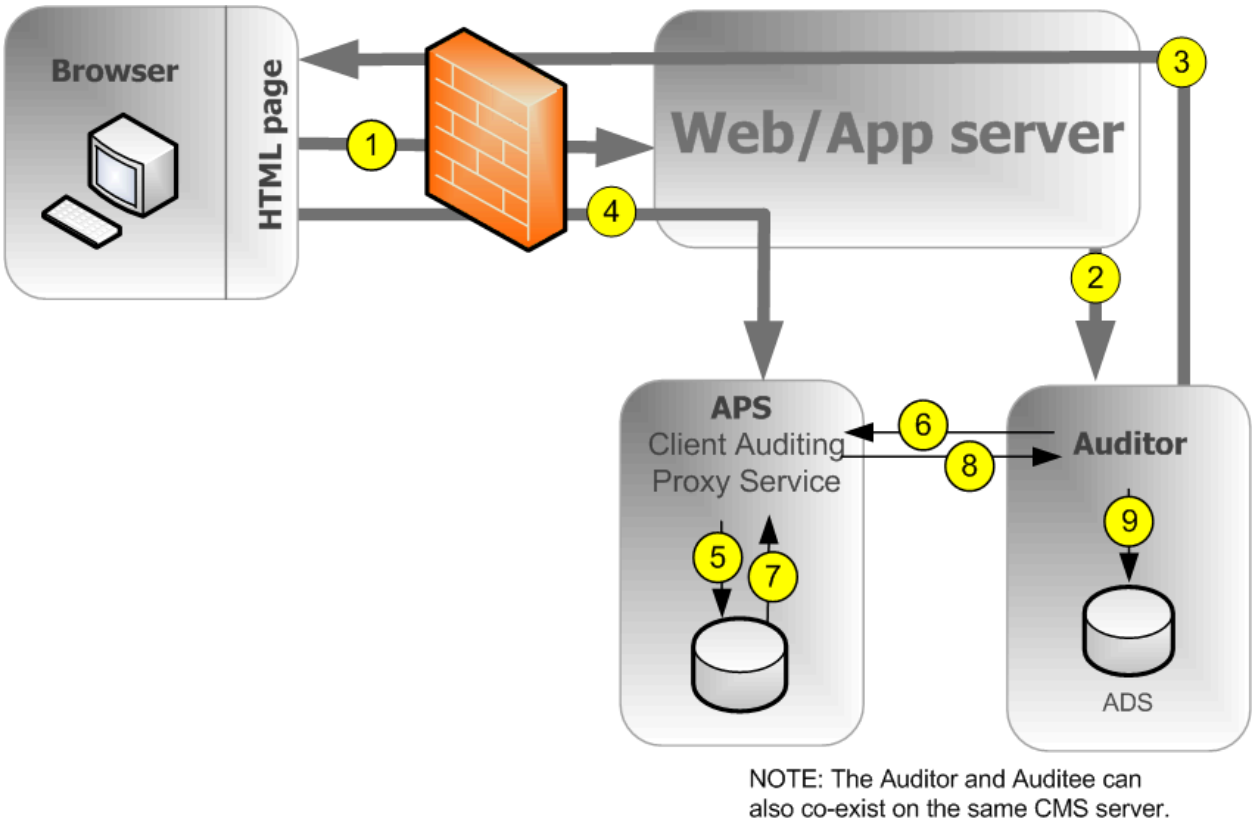
   > **Note**
   >
   > A port in the firewall should be opened between each client and any Adaptive Processing Servers that hosts a CAPS, and also between each client and the CMS. More details on firewalls can be found in the security chapter of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.

5. The CAPS writes events in a temporary file. Steps 1 to 5 can occur multiple times before step 6.
6. At regular intervals, the Auditor polls the CAPS and requests a batch of auditing events.
7. The CAPS retrieves the events from the temporary files.
8. The CAPS sends the event information to the auditor.
9. The auditor writes events to the ADS and signals the CAPS to delete the events from the temporary files.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Non-login auditing for clients connecting through HTTP

This workflow applies to auditing SAP BusinessObjects Web Intelligence events (except for logon events) when connecting through HTTP.



1. The user initiates a potentially auditable event. The client application contacts the web application server.
2. The web application checks to see if the event is configured to be audited.

   > **Note**
   >
   > The diagram shows the Auditor CMS being contacted, but any CMS in the cluster can be contacted for this information.

3. The CMS returns the audit configuration information to the web application server, which passes this information back to the client application.
4. If the event is configured to be audited, the client sends the event information to the web application server, which passes it to the Client Auditing Proxy Service (CAPS), hosted in an Adaptive Processing Server (APS).
5. The CAPS writes events in a temporary file. Steps 1 to 5 can occur multiple times before step 6.
6. At regular intervals, the auditor polls the CAPS and requests a batch of auditing events.
7. The CAPS retrieves the events from the temporary files.
8. The CAPS sends the event information to the auditor.
9. The auditor writes events to the ADS and signals the CAPS to delete the events from the temporary files.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 Rich Client
- Dashboards & Presentation Design
- Analysis Applications
- SAP BusinessObjects Design Studio version 1.3 and later

> **Note**
>
> At least one instance of CAPS must be running in order to collect auditing events from the clients listed above.

Clients not listed above do not directly generate events, but some actions performed by the servers as a result of client application operations can be audited.

Auditing consistency

In most cases, where auditing is properly installed, configured, secured, and correct versions of all client applications are used, auditing will properly and consistently record all indicated system events. It is important to keep in mind, however, that certain system and environment conditions can adversely affect auditing.

There is always a delay between the time an event occurs and its final transfer to the ADS. Conditions such as the unavailability of the CMS or auditing database or loss of network connectivity can increase these delays.

As a system administrator, you should work to avoid any of the following conditions, which could result in incomplete auditing records:

- A drive where auditing data is stored reaches maximum capacity. You should ensure plenty of disk space is available for your auditing database and auditee temporary files.
- An auditee server is improperly removed from the network before it can transmit all audit events. You should ensure that when removing a server from the network, sufficient time is allowed for audit events to post to the auditing database.
- The deletion or modification of auditee temporary files.
- A hardware or disk failure.
- Physical destruction of an auditee or auditor host machine.

There are also some conditions where audit events may be prevented from reaching the CMS-Auditor. These can include:

- Users with older client versions.
- Transmission of auditing information may be blocked by improperly configured firewalls.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Events generated by client applications contain information submitted from the client side, in other words outside the trusted area of the system. Therefore under some conditions this information may not be as reliable as information recorded by the system servers.

> **Note**
>
> If you want to remove a server from your deployment, you should first disable that server but keep it running and connected to your network until all the events in the temporary files have had a chance to transfer to the auditing database. The server's *Current Number of Auditing Events in the Queue* metric will show how many auditing events are waiting to be transferred. When this metric reaches zero, you can stop the server. The location of the temporary files is defined by the `%DefaultAuditingDir%` placeholder for that node. See the Server Administration chapter for more details on placeholders.

> **Note**
>
> If you are going to use Client Auditing it is recommend that you create a dedicated Adaptive Processing Server for the Client Auditing Proxy Service. This will ensure your best system performance. To increase your system's fault tolerance you may also want to consider running the CAPS on more than one APS.

Related links

Server and node placeholders [page 921]

21.2 CMC Auditing page

The *Auditing* page in the CMC has the following areas:

- *Status Summary*
- *Set Events*
- *Set Event Details*
- *Configuration*

21.2.1 Auditing Status

The Auditing *Status Summary* shows a set of metrics that help you optimize your auditing configuration and alert you to any issues that might affect the integrity of your auditing data. The status summary is at the top of the *Auditing* page in the Central Management Console.

The summary will also display warnings under the following circumstances:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- The connection to the Auditing Data Store (ADS) database is unavailable.
- There is no running or enabled Client Auditing Proxy Service, which prevents client events from being collected.
- An auditee has events that could not be retrieved (the server or servers affected will be identified). This usually indicates a server was not properly stopped or shut down and still has events in the temporary files.

> **Note**
>
> The status summary metrics are marked green, yellow, or red to indicate the health of the auditing feature.

Auditing Status metrics

Metric	Details
ADS Last Updated on	The date and time the auditor CMS last finished polling the auditees for their auditing events.
Auditing Thread Utilization	The percentage of the polling cycle the auditor CMS spends collecting data from auditees, the remainder is time spent resting between polls. If this reaches 100% the figure will be displayed in yellow, and means the auditor is still collecting data from the auditees when the next poll is due to begin. This may cause delays in the events reaching the ADS. If this is happening frequently or persistently, it is 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.
Last Polling Cycle Duration	Duration of the last polling cycle in seconds. This indicates the maximum delay for event data to reach the ADS during the previous polling cycle. • If under 20 minutes (1200 seconds), the figure will appear on a green background. • If between 20 minutes and 2 hours (7200 seconds), it will appear on a yellow background. • If over 2 hours, it will appear on a red background. If this state persists and you consider the delay too long, it is recommend you either update your deployment to allow the ADS database to receive data at a higher rate (faster network connections or more powerful database hardware for example), or decrease the number of auditing events your system tracks.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Details
CMS Auditor	The name of the CMS currently acting as auditor.
ADS Database Connection Name	The name of the database connection currently used by the auditor CMS to connect to the Auditing Data Store (ADS). For SQL Anywhere, SQL Server, and SAP HANA servers, this will be the name of the ODBC connection. For other database types it will be the database name and connection port, followed by the server name.
ADS Database User Name	The user name the auditor CMS is using to log in to the ADS database.

21.2.2 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 the BI platform, you will need to set up a connection to the database before you configure your auditing events. Without a connection, events will still be collected, but once connected, the events will be written to the ADS. To turn off auditing the level should be set to off. See *Auditing Data Store configuration settings.*

21.2.2.1 To configure auditing events

1. In the Central Management Console, select the *Auditing* tab.
   The *Auditing* page appears.
2. Set the *Set Events* slider to the desired level.
   The following table shows the different settings for the slider and the events captured at each level.

Auditing Level	Events captured
Off	None
Minimal	○ Logon ○ Logout ○ Rights Modification ○ Custom Access Level Modified ○ Auditing Modification

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Auditing Level	Events captured
Default	*Minimal* events, plus: ○ View ○ Refresh ○ Prompt ○ Create ○ Delete ○ Modify ○ Save ○ Search ○ Edit ○ Run ○ Deliver
Complete	*Minimal* and *Default* events plus: ○ Trigger ○ Drill Out of Scope ○ Page Retrieved ○ Promotion Management Configuration ○ Rollback ○ VMS Add ○ VMS Retrieve ○ VMS Check-in ○ VMS Check-out ○ VMS Export ○ VMS Lock ○ VMS Unlock ○ VMS Delete ○ Cube Connection ○ MDAS Session **Note** More events may exist if add-ons are installed.
Custom	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
Query	If set, *Query* event detail (Detail ID 25) will be recorded for any event that queries a database.
Folder Path Details	If set, the following details will be captured: ○ *Object Folder Path (Detail ID 71)* ○ *Top Folder Name (Detail ID 72* ○ *Container folder path (Detail ID 64)*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Detail	Description
Rights Details	If set, the following details will be captured: ○ *Right Added (Detail ID 55)* ○ *Right Removed (Detail ID 56)* ○ *Right Modified (Detail ID 57)*
User Group Details	If set, the following details will be captured: ○ *User Group Name (Detail ID 16)* ○ *User Group ID (Detail ID 15)*
Property Value Details	If set, the *Property Value* event detail (Detail ID 29) 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.

21.2.3 Auditing Data Store configuration settings

If you chose not to set up an auditing database when you installed the BI platform, or you want to change the database location or settings, you can use the following steps to configure the connection to the ADS.

This is also where you can configure how long auditing events will be retained in the database.

If you have performed an upgrade from a previous version of SAP BusinessObjects Enterprise XI 3.x and have installed version 3.x of Business Objects Metadata Manager (BOMM), it is recommended to configure the ADS to use the same database or tablespace as BOMM.

> **Note**
>
> If you are using an existing DB2 9.7 Workgroup as the auditing database then ensure that the database account is configured to have a page size over 8 kB.

21.2.3.1 To configure your Auditing Data Store database settings

1. On the Central Management Console, select the *Auditing* tab.
2. In the *Configuration* area, under the *ADS Database* heading, select the database type you have set up for your auditing data.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

3. In the *Connection Name* field, enter the name of the connection you have configured for the auditing database.

   Table 90:

Database type	Connection name
IBM DB2	service name
Microsoft SQL Server	ODBC DSN
MySQL	`<serverhostname>,<port>,<databasename>`
Oracle	TNS service name
SAP HANA	ODBC DSN
SAP MaxDB	`<serverhostname>,<port>,<databasename>`
Sybase Adaptive Server Enterprise	service name
Sybase SQL Anywhere	ODBC DSN

   a. If you are using a Microsoft SQL database with Windows authentication, enable the *Windows Authentication* option.

4. In the *User Name* and *Password* fields, enter the user name and password you want the auditor CMS to use when logging onto the database.

   When IBM DB2 is installed by the BI platform as the default database, leave the *User Name* and *Password* fields blank.

5. In the *Delete Events Older Than (Days)* field, enter the number of days you want information to remain in the database. (Minimum value 1, maximum value 109,200.)

   > **Caution**
   >
   > Data older than the number of days set here will be permanently deleted from the ADS; it cannot be recovered. You may want to consider periodically moving records to an archive database if you want to maintain long-term records.

6. In the event the database connection is lost, if you want to manually reconnect the auditor-CMS to the database, de-select the *ADS Auto Reconnect* option.

   > **Note**
   >
   > If this is unchecked, you will need to manually re-establish a connection to the ADS if the connection is lost. This can be done by restarting the CMS, or enabling *ADS Auto Reconnect*. Events will be recorded and remain stored in the temporary files until the ADS is reconnected.

7. Click *Save*.
8. Restart all CMSs in the cluster.

   > **Note**
   >
   > The *Status Summary* at the top of the page shows the current ADS values, which can be different from the values in the *ADS Database* section until the CMSs are restarted.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

21.3 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	The system's auditing settings are modified. • Central Management service
Create	A new object is added to the system. • Central Management Service • Crystal Reports Viewing and Modification Service • Desktop Intelligence • Information Engine Service • Lifecycle management • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
Cube Connection	An OLAP Cube Connection operation is performed. • Multi-Dimensional analysis service • Analysis Applications
Custom Access Level Modified	Information for privileges are modified. • Central Management service
Delete	An object is removed from the system. • Central Management service • Lifecycle Management service
Deliver	An object is sent/delivered to a destination. • Authentication Update Scheduling Service • Central Management Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Desktop Intelligence • Destination Delivery Scheduling Service • Platform Search Scheduling Service • Probe Scheduling Service • Program Scheduling Service • Security query scheduling service • Users and Groups Import Scheduling Service • Web Intelligence Scheduling and Publishing Service
Drill out of scope	A user of a Web Intelligence document has drilled down to a detail level outside the report's pre-loaded data. • Web Intelligence • Web Intelligence Processing Service

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event	Description, and servers and clients that generate the event type
	• Web Intelligence Common Services • Web Intelligence Core Services • Information Engine Service
Edit	The content of an object is changed. • BI Workspaces Application • Desktop Intelligence • Information Engine Service • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
LCM Configuration	The configuration details of Lifecycle Management Console (LCM) are changed. • Lifecycle Management
Logon	A user logs onto the system. • Central Management service
Logout	A user logs out of the system. • Central Management service
Modify	The file properties of an object are changed. • Web Intelligence • Lifecycle Management • Central Management service
MDAS Session	A multi dimensional analysis services operation is performed • Multi-Dimensional analysis service
Page Retrieved	An SAP BusinessObjects Web Intelligence client retrieves additional information from the repository. • Web Intelligence processing service • Web Intelligence Common Services • Web Intelligence Core Services • Information Engine Service
Prompt	Information is entered for a object prompt. • Crystal Reports Cache Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Dashboards Cache Service • Desktop Intelligence • Information Engine Service • Live Office • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event	Description, and servers and clients that generate the event type
	• Web Intelligence Processing Service
Refresh	The data in an object is updated from the database at a user's request. • Crystal Reports Cache Service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Dashboards Cache Service • Desktop Intelligence • Information Engine Service • Live Office • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
Retrieve	An object is retrieved from the repository. • Central Management service • Desktop Intelligence
Rights Modification	The security information is changed for a user, group, or object. • Central Management service
Rollback	LifeCycle Manager is used to revert an object to a previous version. • Lifecycle Management
Run	A job is run. • Authentication update scheduling service • Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Desktop Intelligence • Destination Delivery Scheduling Service • LCM Scheduling Service • Lifecycle management • Platform Search Scheduling Service • Probe Scheduling Service • Program Scheduling Service • Publication Scheduling Service • Replication Service • Security query scheduling service • Users and Groups Import Scheduling Service • Visual Difference Scheduling Service • Web Intelligence Scheduling and Publishing Service
Save	An object is saved after being updated or changed. • Analysis edition for OLAP • Crystal Reports Cache Service

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event	Description, and servers and clients that generate the event type
	• Crystal Reports for Enterprise Scheduling Service • Crystal Reports Scheduling Service • Crystal Reports Viewing and Modification Service • Dashboards • Desktop Intelligence • Information Engine Service • Lifecycle management • Multi-Dimensional Analysis Service • SAP BusinessObjects Mobile • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
Search	A search is performed. • Search service • Explorer • Lifecycle management
Trigger	A file event is triggered. • Event service • Central Management service
View	An object is Viewed. • Analysis Applications • Analysis edition for OLAP • BI launch pad • BI Workspaces Application • CMC • Crystal Reports Cache Service • Crystal Reports Viewing and Modification Service • Dashboards Cache Service • Desktop Intelligence • Information Engine Service • Open Document • SAP BusinessObjects Mobile • Web Intelligence • Web Intelligence Common Service • Web Intelligence Core Service • Web Intelligence Processing Service
VMS Add	An object is added to the LCM Version Management System. • Lifecycle Management
VMS Check in	An object is checked into the LCM Version Management System. • Lifecycle Management

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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. • Lifecycle Management
VMS Export	A resource is exported from the VMS. • Lifecycle Management
VMS Lock	A resource in the VMS is locked. • Lifecycle Management
VMS Unlock	A resource in the VMS is unlocked. • Lifecycle Management
VMS Retrieve	An object is retrieved from the LCM Version Management System. • Lifecycle Management
VMS Delete	An object is deleted from the LCM Version Management System. • Lifecycle Management

Events by Service-type

Service type	Event types generated
Analysis Applications	• View • Cube connection
Authentication Update Scheduling Service	• Deliver • Run
BI Launch Pad	View
Central Management Service	• Auditing Modification • Create • Custom Access Level Modified • Delete • Deliver • Logon • Logout • Modify • Retrieve • Rights Modification • Trigger
Central Management Console	View
Crystal Reports Scheduling Service	• Deliver

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service type	Event types generated
	• Prompt • Refresh • Run • Save
Crystal Reports Cache Service	• Prompt • Refresh • Save • View
Crystal Reports for Enterprise Scheduling Service	• Deliver • Prompt • Refresh • Run • Save
Crystal Reports Scheduling Service	• Deliver • Prompt • Refresh • Run • Save
Crystal Reports Viewing and Modification Service	• Create • Save • View
Dashboards Cache Service	• Prompt • Refresh • View
Dashboards Application	• Save
Desktop Intelligence (client)	• Deliver • Prompt • Retrieve • Run
Desktop Intelligence scheduler process	• Deliver • Run
Destination Delivery Scheduling Service	• Deliver • Run
Event Service	Trigger
Information Engine Service	• Create • Drill out of scope • Edit • Page retrieved • Prompt • Refresh

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service type	Event types generated
	• Save • View
LCM Scheduling Service	Run
LCM service	• Create • Delete • LCM configuration • Modify • Rollback • Run • Save • VMS Add • VMS Checkin • VMS Checkout • VMS Delete • VMS Export • VMS Lock • VMS Retrieve • VMS Unlock • Search
Live Office	• Prompt • Refresh
Multi-Dimensional Analysis Service	• Cube Connection • MDAS Session • Save
OpenDocument	View
Platform Search Scheduling Service	• Deliver • Run
Platform Search Service	Search
Probe Scheduling Service	• Deliver • Run
Program Scheduling Service	• Deliver • Run
Publication Scheduling Service	Run
Replication Service	Run
SAP BusinessObjects Design Studio version 1.3 and later	• Logon • Logoff
Security Query Scheduling Service	• Run • Deliver
Users and Groups Import Scheduling Service	• Run

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Service type	Event types generated
	• Deliver
Visual Difference Scheduling Service	Run
Web Intelligence Application	• Create • Drill out of scope • Edit • Modify • Prompt • Refresh • Save • View
Web Intelligence Common Service	• Create • Drill out of scope • Edit • Page retrieved • Prompt • Refresh • Save • View
Web Intelligence Core Service	• Create • Drill out of scope • Edit • Page retrieved • Prompt • Refresh • Save • View
Web Intelligence Processing Service	• Create • Drill out of Scope • Edit • Page Retrieved • Prompt • Refresh • Save • View
Web Intelligence Scheduling and Publishing Service	• Deliver • Run

Event properties and details

Each event that is recorded by the BI platform includes a set of event properties and details.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event properties will always be generated with an event, although some may not have values if the information is not applicable to a specific event. In the ADS, event properties are included in the table that stores the event, so they can be used to sort or group events when you create reports.

Event details record additional information about the event that is not included in the event's properties. If an event detail is not relevant to a specific event, that event detail will not be generated. There is a set of common event details that can be generated for all event types when they are relevant. There are also sets of additional event details which are generated for specific event types. For example, Prompt events record the values entered for the prompt in an event detail, but no other event type generates a prompt value event detail. In the ADS, details are stored on a separate table which is linked to the parent event.

In some cases, event details can contain multiple values. These details can be grouped using the bunch ID. See the related topic for more information about bunch IDs.

Any multilingual data (such as object or folder names) will be recorded in the default language for the locale of the auditor CMS.

Related Information

Auditing Data Store Tables [page 929]

21.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> **Note**
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> **Note**
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

Event Property	Description
Event_ID	A unique identifier for the event.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event Property	Description
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	CUID of the object affected (if applicable). CUID of the alerting event for Trigger events. **Note** All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need to use the Object_Name property to differentiate these objects.
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast`
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`.
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`.
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.
Parent Document ID	12	• For a document instance: the CUID of the parent document. • For parent documents: its own CUID.
Universe ID	13	CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used.
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.

Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

View

User viewed a document / object.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Event Type ID: 1002

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

> **Note**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. **Note** For View on Demand Crystal Reports this will be set to 0.
Number of Rows	63	The number of records the database server returned. **Note** For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event Detail	ID	Description
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 Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

Create

User created an object.

- Event Type ID: 1005

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event Detail	ID	Description
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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event Detail	ID	Description
		locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on 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).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event Detail	ID	Description
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be reattempted
  - "3" indicates the job was cancelled

Event Detail	ID	Description
Size	17	Size of the document (in bytes) that was run.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Deliver

An object was delivered.

- Event Type ID: 1012

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Event Detail	ID	Description
		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.
Account Name	45	This records one of the following: • For *Inbox* delivered objects, a list of BusinessObjects user account names. • For *FTP* delivered objects, the FTP account name. • For *Unmanaged Disk* delivered objects, the login account used. • For *SMTP* delivered objects, the login account used for the SMTP server.
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	75	Indicates how the delivery was initiated: • "0" indicates scheduled • "1" indicates sent to a destination • "2" indicates published • "3" indicates an alert was triggered

Retrieve

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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.
Client hostname reported by client	51	Hostname of client as reported by client.
Client hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value will be recorded.
Client IP address reported by client	53	IP address of client as reported by the client.
Client IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value 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: 1016

Event Detail	ID	Description
File Name	18	The name of the file that was being monitored and triggered the event.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

21.3.1.1 Platform events

The following events are specific to the BI platform.

Rights Modification

Right or rights for an object were modified.

- Event Type ID: 10003

Event Detail	ID	Description
Rights Added	55	The type of right added, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types.`
Rights Removed	56	The type of right removed, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types.`
Rights Modified	57	The type of right modified, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types.`
Principal	118	The ID of a user or user group (principal) for whom security rights were modified.
Principal Name	119	The name of a user or user group (principal) for whom security rights were modified.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Custom Access Level Modified

A Custom Access Level was modified.

- Event Type ID: 10004

Event Detail	ID	Description
Rights Added	55	The type of right added, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
Rights Removed	56	The type of right removed, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types.`
Rights Modified	57	The type of right modified, the scope of the new right (which objects) and the object type it was applied to. The information will be structured according to the following example: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types.`
Principal	118	The ID of a user or user group (principal) for whom security rights were modified.

Auditing Modification

A change was made to the system's auditing settings.

- Event Type ID: 10006

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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	78	If the connection to the Auditing Data Store is changed, this records the new connection settings using the following format: `DBType=Oracle,DBName=MyADS,Username=USR1,Password="******",SSO=off,DBReconnect=on`. Only the details changed will be recorded. For example, if the user name is the only thing updated, then only `Username="new"` will be recorded. **Note** The password information will always be obscured with * in the database.
Auto Delete Interval	105	This detail will record any changes to the *Delete Events Older Than* field in the Auditing CMC page. This governs how many days auditing information will be maintained in the ADS.

21.3.1.2 SAP BusinessObjects Web Intelligence events

The following events are specific to the SAP BusinessObjects Web Intelligence component.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Drill Out Of Scope

User drilled out of the report's scope.

- Event Type ID: 10201

Event Detail	ID	Description
Object Instance	11	Records if the event is the result of a scheduled update or a user viewing the object ("0" = resulted from a user viewing the object, "1" = resulted from a scheduled refresh of the object).
Number of Rows	63	The number of rows the database server returned.
Query	25	Records the query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document uses. An instance will be recorded for each universe accessed by the document.
Universe ID	32	The CUID of the universe the document uses. An instance will be recorded for each universe accessed by the document.

Page Retrieved

Web Intelligence document page was retrieved.

- Event Type ID: 10202

21.3.1.3 SAP BusinessObjects Analysis, edition for OLAP events

MDAS Session

An MDAS session operation is performed

- Event Type ID: 10300
- Statuses:
  - "0" = A new session opened successfully.
  - "1" = A new session failed.
  - "2" = An existing session is closed.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

MDAS Cube Connection

A Cube Connection operation is performed.

- Event Type ID: 10301
- Statuses:
  - "0" = A new connection opened successfully.
  - "1" = A new connection failed.
  - "2" = An existing connection is closed.

Event Detail	ID	Description
Connection ID	94	Unique identifier for the connection.
Connection Name	95	The name of the connection.
Provider type	96	The type of provider for the cube.
Cube Name	97	The full name of the cube used.

21.3.1.4 SAP BusinessObjects Promotion Management console events

The following events are unique to the Promotion Management for SAP BusinessObjects component.

SAP BusinessObjects Promotion management tool common details

All Promotion Management events will have the following additional event details.

Event Detail	ID	Description
Element Cluster	6	The CUID of affected clusters when promotion management tool performs an operation on objects located in different clusters. An event detail will be generated for each affected cluster.
Element Comment	7	Additional information on the object.
Primary Element	8	If the element is a primary element, this detail will be set to "1"; if it is a dependent element, it will be set to "0".
Element Status	9	If the operation element fails this detail will be set to "1"; otherwise it will be "0".
Operation	10	Describes the type of operation performed (for example Add, Delete, or Modify).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP BusinessObjects Promotion management tool Configuration

Configuration of Promotion Management is changed.

- Event Type ID: 10900

Event Detail	ID	Description
Configuration	100	A user views the promotion management tool configuration. The configuration displays as comma-separated value pairs, for example: rollback settings=enabled, port=900.
Configuration Before	101	If the promotion management tool settings for an object are modified, records the previous configuration settings. Uses the same format as Configuration.
Configuration After	102	If the promotion management tool settings for an object are modified, records the new configuration settings. Uses the same format as Configuration.
VMS Type	10900	The type of version management system.

Rollback

An object was rolled back to a previous Version Management System (VMS) version.

- Event Type ID: 10901

VMS Add

A resource is added to the VMS.

- Event Type ID: 10902

Event Detail	ID	Description
Version	104	Records the version number of the document in the Version Management System.

VMS Retrieve

A resource is retrieved from the VMS.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

VMS Lock

A resource in the VMS is locked, to prevent users editing it.

- Event Type ID: 10907

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.
Locked By	10901	The user name of the user who performed the action.

VMS Unlock

A resource in the VMS is unlocked, allowing users to edit it.

- Event Type ID: 10908

Event Detail	ID	Description
Version	104	Records the version number of the document in the VMS.
Unlocked By	10902	The user name of the user who performed the action.

VMS Delete

A resource is deleted from the VMS.

- Event Type ID: 10909

Event Detail	ID	Description
Version	104	Records the version number of the document in the Version Management System.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

22 Platform Search

22.1 Understanding Platform Search

Platform Search enables you to search content within the BI platform repository. It refines the search results by grouping them into categories and ranking them in order of their relevance.

In this version of the BI platform, Platform Search is enhanced with the following features:

- Search for both BI platform and Explorer content.
- Suggest a query for creating a document if it cannot find an existing document.
- Support both continuous and schedule-based indexing.
- Support indexing in a clustered environment.
- Set and modify the level of indexing.
- Provide advanced search configuration options.
- Support multilingual search and indexing.
- Provide an advanced search syntax.
- Support metadata, content, and dynamic facets.
- Support self healing based on the system load.

> **Note**
>
> If you migrate from the previous version to a new version, the index is not migrated.

22.1.1 Platform Search SDK

Platform Search supports a public SDK that functions as an interface between the client application and Platform Search. It is publicly exposed to help you customize the search service and integrate it with your application.

When a search request parameter is sent through the client application to the SDK layer, the SDK layer converts the request parameter into XML-encoded format and passes it to the Platform Search Service.

For more information about the Platform Search API, see the *Business Intelligence platform Java API Reference*.

22.1.2 Clustered Environment

Platform Search can share the load across multiple nodes in a clustered environment. The deployment in a clustered environment optimizes system resources and enhances server performance.

Platform Search supports both horizontal and vertical clustering for both search and indexing features. With clustered environments, it optimizes the performance of both search and index processes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Load balancing

Platform Search supports load balancing for both indexing and searching. In a clustered environment, indexing and search requests can be executed on multiple nodes to share the load. Each node functions independently to index the content and create delta indexes. However, only one node in the cluster will act as a master index and merge the delta indexes into the master index. All nodes can access the master index. This enables simultaneous search requests.

Failover

The failover mechanism ensures that users can continue to search and use the index operation without disruption. When a node in the cluster becomes unavailable due to a technical failure or maintenance-related activities, another node automatically takes over the process of indexing and searching requests.

22.2 Setting Up Platform Search

22.2.1 Deploying OpenSearch

Platform Search supports the OpenSearch standard, enabling client applications to use the OpenSearch standard or format to communicate with Platform Search. OpenSearch is not installed by default with the SAP BusinessObjects Business Intelligence suite, so users need to deploy it manually as a separate WAR file (`opensearch.war`) to an application server such as Tomcat, or using the WDeploy tool. This file is copied into the **<INSTALLDIR>**`\warfiles\OpenSearch` directory by the installer.

> **Note**
>
> Client programs need to follow the OpenSearch standards to communicate with Platform Search.

> **Note**
>
> When you install the BI platform, the Tomcat application server is installed by default.

22.2.1.1 Deploying Manually

To deploy OpenSearch in a BI platform environment, perform the following steps:

1. Go to the following location: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Copy the OpenSearch folder into **<INSTALLDIR>**`\tomcat\webapps\`.
3. Change the configuration parameters in the `\OpenSearch\WEB-INF\config.properties` file:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- CMS: the CMS name with port number: `<CMS Name>:<Port Number>`.
- OpenDocURL: the URL of the OpenDocument application: `http://<tomcathost>:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp`.
- Proxy.rpurl: the reverse proxy server name is required if you want to use reverse proxy.
- Proxy.opendoc.rpurl: the opendoc reverse proxy server name is required if you want to use the reverse proxy.

4. Restart the Tomcat application server to deploy OpenSearch.

22.2.1.2 Deploying using WDeploy

For Windows, commands are described as `wdeploy.bat <parameters>`. For UNIX, commands are described as `wdeploy.sh <parameters>`.

1. Update the `config.`**`<ApplicationServer>`** file located at **`<InstallDir>`**`\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` with the required web application server parameters (for example, installation directory, instance name, administrator port, administrator user name, and administrator password).
2. Change the following parameters in the **`<InstallDir>`**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties` file:
   a. For the CMS parameter, enter **`<CMSName>`**:**`<Port>`**.
   b. For the OpenDocURL parameter, enter the URL of the OpenDocument application.
      The URL should be `http://`**`<WebApplicationServerHost>`**`:`**`<ConnectorPort>`**`/BOE/OpenDocument/opendoc/openDocument.jsp`.
   c. (Required for reverse proxy) For the Proxy.rpurl parameter, enter the reverse proxy server name.
   d. (Required for reverse proxy) For the Proxy.opendoc.rpurl parameter, enter the OpenDocument application's reverse proxy server name.
3. Execute the wdeploy.bat **`<WebApplicationServer>`** -Dapp_source_tree=**`<ParentFolderOpenSearchWebApp>`** -DAPP=OpenSearch deploy command from **`<InstallDir>`**`\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   For example, the following command deploys OpenSearch to a WebSphere 7 web application server:

```
wdeploy.bat websphere7 -Dapp_source_tree="<InstallDir>\SAP BusinessObjects
Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```

4. Restart the web application server.

22.2.2 Configuring reverse proxy

To deploy web applications on a Web application server located behind the reverse proxy server, configure a reverse proxy server to map incoming URL requests to the correct WAR file.

To illustrate the configuration steps, we use Apache 2.2 Reverse Proxy server as an example. To configure Apache 2.2 Reverse Proxy server for OpenSearch:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Set up the reverse proxy and make the changes in the `WEB-INF\config.properties` file of OpenSearch.
2. Enable the following context parameters and change the values accordingly.
   - `proxy.rpurl`: This is the reverse proxy URL for OpenSearch (such as `http://machineIPAddress/RP/OpenSearch/`).
   - `proxy.opendoc.rpurl`: This is the reverse proxy URL for Open Doc (such as `http://machineIPAddress/RP/BOE/`).
3. Update the `httpd.conf` file, located under the Apache Reverse Proxy installation folder, with the following settings:
   - `ProxyPass /RP/BOE/OpenDocument/ http://<Tomcat host>:<Connector Port>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<Tomcat host>:<Connector Port>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Restart the Apache 2.2 Reverse Proxy server.

22.2.3 Configuring Application Properties in the CMC

To configure the Platform Search application properties, complete the following steps:

1. Go to the *Applications* area of the CMC.
2. Select *Platform Search Application*.
3. Click *Manage* > *Properties*. The *Platform Search Application Properties* dialog box appears.
4. Configure the Platform Search settings:

Table 91:

Option	Description
Search Statistics	Platform Search offers the following search statistics: ○ Indexing Status: displays the status of the indexing process. ○ Number of indexed documents: displays the number of documents that are indexed. ○ Last indexed time stamp: displays the time stamp at which the document was last indexed.
Stop / Start Indexing	Start or Stop Indexing options enable you to start or stop the indexing process when you want to switch from continuous crawling to scheduled crawling, or for maintenance purposes. To stop indexing, click *Stop Indexing*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Default Index Locale	Platform Search uses the locale specified in the CMC for indexing all the non-localized BI documents. Once the document is localized the corresponding language analyzer is used for indexing. Search is based on the client's product locale, and the weighting is given to the client's product locale. You can configure the weighting in the CMC configuration properties.
Crawling Frequency	You can index the entire BI platform repository by using the following options: ○ Continuous crawling: With this option, indexing is continuous; the repository is indexed whenever an object is added, modified, or deleted. It allows you to view or work with the most up-to-date BI platform content. Set by default, continuous crawling updates the repository continuously with the actions that you perform. Continuous crawling works without user intervention, and reduces the time taken for indexing a document. ○ Scheduled crawling: With this option, indexing is based on the schedule set by the Schedule options. For more information about scheduling an object, refer to the *Scheduling an Object* section of Platform Search in the *SAP BusinessObjects Business Intelligence platform CMC Online Help*. **Note** ○ If you select *Scheduled Crawling* and set the *Recurrence* to an option other than *Now*, Platform Search displays the date and time stamp when the document is scheduled to be indexed next. ○ If you select *Scheduled Crawling*, then the *Start Indexing* button is enabled and the *Stop Indexing* button is disabled. ○ Once the scheduling is complete, the *Stop Indexing* button is disabled.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Index Location	The indexes are stored in shared folders in the following locations: ○ Master index location (indexes and speller): The master and speller indexes are stored in this location. During a search, the initial results are retrieved using the Master Index, and the speller indexes are used to retrieve suggestions. In a clustered BI platform deployment, this location should be on a shared file system that is accessible from all nodes in the cluster. ○ Persistent data location (Content stores): The content store is placed in this location. It is created from the master index location and remains synchronized with it. The content store is used to generate facets and process the initial hits generated from the Master Index location. In a clustered BI platform deployment, content stores are generated at every node. The persistent data location is the only index location that is affected by the clustered environment as it contains the content store folders. If a machine has a single search service, then there will be only one content store location. For example, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. However, in a clustered environment, if there are multiple search services, then each search service will have one content store location. For example, if you have two instances of a server running, then the content store locations would be as follows: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name 1>\ContentStores. ○ Non-persistent data location (Temporary files, Delta Indexes): In this location, the delta indexes are created and stored temporarily before being merged with the Master index. The indexes at this location are deleted once they are merged with the Master Index. In addition, surrogate files (output of the extractors) are created in this location and stored temporarily until they are converted into delta indexes. **Note** ○ Master index location must be a shared location. ○ You need to click *Stop Indexing* to modify the index location. ○ If you modify an index location, copy the content to a new location, or the existing index information will be lost.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description

Level of indexing	You can tune the search content by setting the level of indexing in the following ways:
	○ Platform Metadata: An index is created only for the platform metadata information such as titles, keywords, and descriptions of the documents. By default, this option is selected.
	○ Platform and Document Metadata: This index includes the platform metadata as well as the document metadata. The document metadata includes the creation date, modification date, and name of the author.
	○ Full Content: This index includes the platform metadata, document metadata, and other content such as:
	  ○ The actual content in the document
	  ○ The content of prompts and LOVs
	  ○ Charts, graphs, and labels
	Note
	Full content indexing is not supported for Analysis Office and Lumira documents. Only metadata indexing is supported for Analysis Office and Lumira documents.
	Note
	When you modify the level of indexing, the indexing is initialized for the entire BI platform repository refresh.

Content Types	You can select the following content types for indexing: ○ Crystal Reports ○ Web Intelligence ○ Universe ○ BI Workspace ○ Analysis Office ○ Lumira ○ Microsoft PowerPoint ○ Adobe Acrobat ○ Rich Text ○ Text ○ Microsoft Word ○ Microsoft Excel The content type filter does not apply for platform metadata indexing. Regardless of the content types you select, platform metadata indexing happens for all the supported object types and the search results in BI launch pad returns all the objects for the keyword related to platform metadata. The content type filter is relevant for document metadata indexing (document author, document header, document footer, and so on) and content indexing (graphs , charts , table with a report). Based on the level of indexing and content types you select, platform search indexes the document metadata and content for the selected objects types from the repository and only those objects appear in the BI launch pad search results, when searching for keyword related to document metadata and content.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Rebuild index	This option deletes the existing index and re-indexes the entire repository. You can select the *Rebuild index* option whether indexing is running or stopped. The existing index is deleted when you save your changes to the properties page. However, if indexing is currently stopped, the index does not start rebuilding until you restart indexing. If you do not want Platform Search to re-index the documents, clear the *Rebuild index* option before clicking *Start Indexing*.
Documents Excluded from Indexing	The *Documents Excluded from Indexing* option excludes documents from indexing. For example, you may not want extremely large Crystal reports to be made searchable to ensure the report application server resources are not overloaded. Similarly, you may not want publications with hundreds of personalized reports to be indexed. By excluding particular documents, you can prevent them from being accessed by Platform Search. It is important to note that if a document is already indexed before it is put into this group, the document may still be searchable. To ensure that documents in the *Documents Excluded from Indexing* group are not searchable, you must rebuild the index. By default, only the Administrator account has full control of the *Documents Excluded from Indexing* option. Other users with the following rights can only add documents to the *Documents Excluded from Indexing* group: ○ View and edit rights on the category ○ Edit the document directly

5. Click *Save & Close*.

> **Note**
>
> If a user does not select the *Rebuild Index* option and changes the level of indexing or selects or deselects extractors, then the index is incrementally updated without deleting the existing index.

22.3 Working with Platform Search

22.3.1 Indexing Content in the CMS Repository

Indexing is a continuous process that involves the following sequential tasks:

1. Crawling: Crawling is a mechanism that polls the CMS repository and identifies objects that are published, modified, or deleted. It can be done in two ways: continuous and scheduled crawling.
   For more information on continuous and scheduled crawling, refer to the *Configuring Application Properties* topic in Related Topics.
2. Extracting: Extracting is a mechanism to call the extractors based upon the document type. There is a dedicated extractor for every document type that is available in the repository. New document types can be made searchable by defining new extractor plug-ins. Each of these extractors is scalable enough to extract content from large documents that contain many records.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The following extractors are supported:

- Metadata extractor
- Crystal report extractor
- Web Intelligence extractor
- Universe extractor
- Agnostic extractors (MS Office 2003 and 2007 and PDF documents)

For more information on searchable document types, refer to the *Searchable content types* topic in Related Topics.

3. Indexing: Indexing is a mechanism that indexes all the extracted content through a third-party library, called Apache Lucene Engine. The time required for indexing varies, depending on the number of objects in the system, and the size and type of documents.
   For indexing to run successfully, the following servers must be running and enabled:
   - Input File Repository Server (IFRS)
   - Output File Repository Server (OFRS)
   - Central Management Server (CMS)
   - The Adaptive Processing Server (APS) that hosts the Platform Search service

   If the object type is selected as Web Intelligence or Crystal report, the corresponding Web Intelligence Processing Server or Crystal Reports Application Server must be running and enabled for the respective object types selected.
4. Content Store: The content store contains information such as id, cuid, name, kind, and instance extracted from the main index in a format that can be read easily. This helps to quicken the search process.

Related Information

Configuring Application Properties in the CMC [page 568]
Searchable Content Types [page 679]

22.3.2 Indexing Failure Listing

The indexing failure listing provides a list of documents that fail to get indexed. platform Search offers three attempts for a document to get indexed. If a document fails to get indexed, it is listed in the indexing failure listing.

To view the indexing failure listing, complete the follwoing steps:

1. Go to the "Applications" area of the CMC.
2. Select *Platform Search Application*.
3. Choose*Actions > Indexing failure listing*.

   The "Platform Search Application" dialog box appears, displaying a list of documents with the following details:
   - Title: displays the title of the document that failed to get indexed.
   - Type: displays the name of the document type, such as Crystal Report and Web Intelligence, and the location of the document.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Failure Type: displays the error code and the reason for index failure of the document. Click the More info hyperlink to learn more about the stack trace of the cause of the error.
- Last attempted time: displays the time stamp of the last attempt to index a document.

22.3.3 Searching Results

22.3.3.1 Pre- Search

22.3.3.1.1 Suggested Queries

When using Platform Search, a user may be trying to find answers to a specific question rather than looking for a specific object. These questions may or may not be answered in reports available in the BI platform repository.

Platform Search analyzes the structure of universes and existing reports in your repository and compares this information to the search request that the user has provided to suggest new SAP BusinessObjects Web Intelligence queries that may help users find the answers to their questions.

To create potential reports, Platform Search matches the words in all universes for dimension, measure, condition and filter value.

Platform Search looks for matches in the following information about universes or existing Web Intelligence documents:

- Measures in universes that match words in the search input.
  When a measure matches one of the search terms, that measure will be used in the resulting Web Intelligence document.
- Dimension names in universes that match words in the search input.
  When a dimension name matches one of the search terms, the resulting Web Intelligence document breaks down the information on this dimension.
- Query filters may be used to focus the data shown in the document. These query filters are generated by analyzing the search input.
  - If the name of a universe condition matches one of the search terms, the condition is used as the filter.
  - If there are field values in existing Web Intelligence documents whose names match search terms, a filter will be created from the dimension from the historical report with the matched value, using "equal to" as the condition operator.

If Platform Search has made enough matches that the resulting document will contain two result fields and one filter, the query is considered to be ready to run. In this case, the user can click to view the completed report.

If there are insufficient number of matches between universes and the document, you can edit the query before running it.

Platform Search suggests multiple queries if several universes matches the search input, or if the same word appears in two different matches, such as in the name of a dimension and as a filter value.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

22.3.3.1.2 Searchable Content Types

The content published to the BI platform is searchable with Platform Search. The object types are listed below with their corresponding indexed content:

Table 92:

Object Type	Indexed Content
Crystal Reports (2008, 2011, and 2013)	Title, description, selection formula, saved data, text fields in any section, parameter values, and sub-reports.
Web Intelligence documents	Title, description, name of the universe filters used in the report, saved data, constants in the filter condition locally defined in the report, name of the universe measures used in the report, name of the universe objects used in the report, data in record set, and static text in cells.
Microsoft Excel documents (2003 and 2007)	Data in all non-empty cells, fields on the Summary page of the document properties (title, subject, author, company, category, keywords and comments), and text in document headers and footers. For cells that use calculation or formula, the value after the evaluation is searchable. For number or date/time values, the raw data is searchable.
Microsoft Word documents (2003 and 2007)	Text in all paragraphs and tables, fields on the Summary page of the document properties (title, subject, author, company, category, keywords and comments), text in document headers and footers, and numerical text.
RTF, PDF, PPT and TXT Files	All text in these files is searchable.
LCMJob, AFDashboard Page, Dashboards, ObjectPackage, Web service query (QaaWS), Profile, Discussions, InformationDesigner, widgets for SAP BusinessObjects BI platform, MDAnalysis, Publications, Flash, Analytic and Hyperlink	Metadata content is searchable.
Events	All events such as Custom events, System events, Crystal Reports events and Monitoring events are searchable. If an event is associated with a source, Platform Search surfaces the source along with the event. **Note** Platform Search supports events for Crystal Reports for Enterprise.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object Type	Indexed Content

BI Workspace	• The title, description, and contents of the following BIW modules are indexed:
	  ○ Text module
	  ○ Web Page module
	  ○ Navigation List module
	  ○ Viewer module
	• The title and description of a Compound Module is indexed.
	• Only the title of a Workspace Template Module is indexed.
	• In the case of a Group module, the title and metadata of the modules within it, is indexed.
	• The title, description, and CUID of InfoObject modules in BIW are indexed.
	Note
	Since only the title and description of an embedded InfoObject module is indexed, attempts to search for the InfoObject content, will not return references to the embedded module. For example, if a CR is inserted in BIW, its title and description is indexed. Any attempts to search for the contents of the CR will not return references to the embedded module.
	• If a BIW contains multiple tabs and sub-tabs, the title and contents of each tab and sub-tab, is also indexed.

CR Next Gen	Title, description, selection formula, saved data, text fields in any section, parameter values, and sub-reports. The following objects in a CR Next Gen report are not supported: • Cross Tab report • Chart data extraction • Images and associated metadata extraction • Embedded OLE (for example, a Word document embedded in CR) • Flash object extraction Also, It is not possible to read data page by page from a CR Next Gen report.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object Type	Indexed Content
Universe	Data content is searchable. **Note** By default, the universe indexing option is enabled. If you notice that queries used by Platform Search to index universe content take a long time to run, and impact database server performance, then we recommend disabling the universe indexing option in the Central Management Console (CMC). An example of a query that Platform Search uses while indexing universe content is *Select distinct SampleColumnName from SampleTableName LIMIT 1000*. Follow these steps to disable universe indexing: 1. Logon to the Central Management Console (CMC). 2. Choose *Applications*. 3. Navigate to Platform Search Applications and choose *Properties*. 4. Navigate to content types and uncheck *Universe*. 5. Choose *Save & Close*.
Lumira document	Only metadata content is searchable.
Analysis Office document	Only metadata content is searchable.

Note

The maximum size supported for Agnostic documents (MS Office 2003 and 2007 and PDF documents) is 15 MB.

22.3.3.2 Search

When a user searches for a keyword from BI launch pad or any other application that uses the Platform Search SDK, the master index is checked for their search terms. Based on the user's view rights, the search engine displays only those documents for which a user has the access rights.

22.3.3.3 Post- Search

22.3.3.3.1 Facets

Platform Search refines the search results by grouping them into categories or facets of similar object types, and ranking them in order of the number of occurrences of the category among the returned results for the search term. Facets enable you to navigate to the exact result.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Platform Search generates facets from InfoObject metadata, document metadata, and document content. It displays only those facets that have more than two documents matching a specified query. Facets are surfaced dynamically based on the documents that match the search query and are sorted by document count.

Documents are grouped into the following generic facets or categories:

- Personal or public (such as HR, Corporate, and Finance): this is based on the BI platform document categories.
- Document type: this is based on the document type such as Web Intelligence, Crystal Reports, Microsoft Word (2003 and 2007), Microsoft Excel (2003 and 2007), and Dashboards.
- Universe and Connections: this is based on the content source.
- Date: this includes the last refreshed date: (year, quarter and month).
- Time: this includes the last refreshed time, such as, 24 hours and last week.
- Author: this is the name of the user who created the document.

> **Note**
>
> When working in Hebrew or Arabic locale, if you search for content objects in BI launch pad, the search result does not display facets.

22.3.3.3.2 Normalizing the Search Results Ranking

Platform search considers the place of occurrence of the searched term when ranking a document. It groups the content into the following categories based on the occurrence of the content in the document:

1. Platform Metadata
2. Document Metadata
3. Content Metadata
4. Content

You can configure the weighting for these categories in the CMC.

22.3.3.3.2.1 Customizing Weight for Ranking Search Results

Platform Search allows you to set weights for the content grouped in categories based on the occurrence of the content in the document, so that you can set a higher value for the desired category to retrieve related search results faster.

To set the weight, perform the following steps:

1. In the *Manage* area of the CMC, click *Applications*.
2. Open *Platform Search Application*.
3. Choose *Ranking*.

   The weights of different content categories such as Platform Metadata, Document Metadata, Content Metadata and Content are shown. The *User locale* is the locale set in the BI launch pad Preferences.
4. Set the weights to meet your requirements.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5. Choose *Save*.

In an upgrade scenario, if ranking needs to be applied for documents that are already indexed, you need to rebuild the index. For more information, refer to information about rebuilding the index in the Configuring Application Properties in the CMC [page 568] section.

22.3.3.3.3 Multilingual Support

Platform Search offers multilingual support to index content, retrieve search results and get suggestions in your desired language. To index all non-localized BI platform documents, it uses the locale set in the *Default Index Locale* in the CMC.

Once the InfoObject is localized, Platform Search uses the corresponding language analyzer to index the document.

Search is based on the locale set as the Client's Product Locale. Platform Search gives more weighting to the Client Product locale while retrieving search results. You can configure the weights in the CMC.

22.3.3.3.4 Suggestions

Platform Search offers suggestions for incorrectly-spelled search queries. If the original search query does not yield any results, then Platform Search suggests the most probable terms based on the indexed content.

Suggestions appear as keywords with a hyperlink. Click a hyperlink to view a list of documents containing the keyword that may match your original query. These suggestions are determined algorithmically based on various objective factors.

If there are multiple terms that may match the original request, Platform Search suggests the top three suggestions in the language set as the *Default Index locale* in the CMC.

> **Note**
>
> Platform Search does not generate suggestions in these cases:
>
> - If the search queries contain fewer than three letters
> - For attributed searches, such as Type: Crystal Report
> - For universe metadata and content
> - For multi-byte languages such as Chinese, Japanese, and Korean

22.3.3.3.5 Federating Search Results from SAP BusinessObjects Explorer

Platform Search federates the search requests from SAP BusinessObjects Explorer and surface InfoSpaces along with the BI platform content.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The search results from SAP BusinessObjects Explorer are grouped by metadata categories. The supported facets for InfoSpaces include type, location, and refresh time.

SAP BusinessObjects Explorer sends the term frequency to Platform Search for each search term in the search query. Platform Search calculates the relevancy using a sum of the square root of the term frequencies. The resultant value is assigned as a score to each InfoSpace. The results are then sorted by score and sent to the client.

22.4 Integrating Platform Search with SAP NetWeaver Enterprise Search

SAP NetWeaver Enterprise Search 7.20 and above can use a search service based on OpenSearch (RSS and ATOM). It can delegate search requests to remote search service provider systems. In this case, OpenSearch is the service provider, SAP NetWeaver Enterprise Search is the search results consumer, and SAP BusinessObjects Platform Search is the search service provider.

If a user submits a search request, SAP NetWeaver Enterprise Search forwards the search request directly to the OpenSearch provider. The provider replies to the search request and sends the reply back to SAP NetWeaver Enterprise Search. It is then merged with the results received from other search object connectors to a search result and displayed on the user interface.

To integrate SAP NetWeaver Enterprise Search and Platform Search, you need to perform the following steps:

1. Create a connector in SAP NetWeaver Enterprise Search.
2. Import a user's role into the BI platform.

22.4.1 Creating a Connector in SAP NetWeaver Enterprise Search

You can use a search object connector of type OpenSearch to integrate external search providers that offer a search function available through OpenSearch.

To create a connector in SAP NetWeaver Enterprise Search, you need the following pre-requisites:

1. The OpenSearch description service URL.
2. The OpenSearch description service must be available in the RSS or ATOM format only.

Perform the following steps to create a connector in SAP NetWeaver Enterprise Search:

1. Launch the administration cockpit and choose Create.
2. Select OpenSearch as the search object connector type.
3. Choose *Next*.
4. Enter the OpenSearch description service URL of the OpenSearch provider.
5. Select any one of the following authentication settings to launch the description service URL:
   - No Authentication: No authentication takes place.
   - SAP Authentication Assertion Ticket: This user is used for authentication via SSO.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- User/Password: A predefined user is used for authentication.

6. Select Launch Search URL from the OpenSearch URL settings.
   The OpenSearch description service is then validated for a suitable search service. The system automatically enters a value for the search URL template and the associated description.
7. Select any one of the following authentication settings to set up a connector:
   - No Authentication: No authentication takes place.
   - SAP Authentication Assertion Ticket: This user is used for authentication via SSO.
   - User/Password: A predefined user is used for authentication.
8. Choose *Next*.
   A summary dialog box appears displaying the values entered for this search object connector.
9. Choose *Previous* to modify the settings, or *Cancel* to discard all the entered data.
10. Choose *Finish* to save the settings.

22.4.2 Importing a User's Role into the BI platform

Perform the following steps to import a user's role into the BI platform:

> **Note**
>
> The administrator must have the user details, system information, and application host information and user credentials.

1. Go to the *Authentication* area of the CMC.
2. Choose *SAP*.
3. Specify the following on the *Entitlement Systems* tab:
   - System
   - Client
   - Application Server
   - System Number
   - Username
   - Password
   - Language
4. Choose *Update*.
5. Choose*Role Import* tab and import user roles.
6. Choose *Update*.
7. Choose *Manage* > *User Security* in the CMC to assign the appropriate user's rights.

22.5 Searching from SAP NetWeaver Enterprise Search

To search results from SAP NetWeaver Enterprise Search, perform the following steps:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

1. Log on to the SAP NetWeaver Enterprise Search application.
2. Choose *Advanced Search*.
3. Select the connector that was created for Platform Search.
4. Search for a keyword.

   Consolidated results for the keyword contain the results from Platform Search if there is a match on the keyword.

22.6 Auditing

All the events of search requests sent from a client application that uses the Platform Search Service and the search response are audited. For Platform Search, the auditing is implemented at the service level.

The Platform Search Service must run with a Client Auditing Proxy Service on the same server in order to send audit events.

There is one Event Type ID 1009 for Platform Search and four Platform Search-specific Event Detail Type IDs:

- Keyword searched (ID: 19)
- Number of Search Results (ID: 63)
- Facet Search (ID: 20)
- Search Exception (ID: 1)

Apart from the above event details, there are a few standard event details like sessionCuid and userCuid which are supported for any auditing in any BI platform module.

How auditing works in Platform Search is explained below with an example.

If you search a keyword such as "Sales", the total number of search results could be 5. In this case, the following events are audited:

- Event Type ID 1009
- Event Detail Type ID 19 with the value sales
- Event Detail Type ID 63 with the value 5
- Session CUID
- User CUID
- Status with value 0 which is success state
- Start time
- Duration
- Object ID with value 0 since this is service-side auditing

When Facets are generated and you select one or more facets, the following events are audited:

- Event Type ID 1009
- Event Detail Type ID 19 with the value sales
- Event Detail Type ID 63 with the value 5
- Event Detail Type ID 20 with comma separated string of facets
- Session Cuid
- User Cuid

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Status with value 0 which is success state
- Start time
- Duration
- Object ID with value 0 since this is service side auditing

If there is a search exception due to an invalid entry (for example *"a"), the following event details are audited:

- Event Type ID 1009
- Event Detail Type ID 19 with the value sales
- Event Detail Type ID 63 with the value 0
- Event Detail Type ID 1 with the exception message
- Session Cuid
- User Cuid
- Status with value 1 which is failure state
- Start time
- Duration
- Object ID with value 0 since this is service side auditing

22.7 Troubleshooting

22.7.1 Self Healing

Platform Search has its own self-healing mechanism. It continuously monitors the search service memory usage and stops indexing automatically when memory usage exceeds the threshold value. It automatically starts after the memory usage reduces to a reasonable limit. However, users can continue to search during this process but cannot index for a specific period of time. By default, Platform Search configures the number of documents that can be indexed at any instant, based on the document type. The indexing is initiated based on the system resources like CPU and memory.

22.7.2 Problem Scenarios

This section provides step-by-step solutions to a wide range of problems that may occur while retrieving search results with Platform Search.

Unable to retrieve search results from the newly added document containing the keyword

- Check if Platform Search supports the document type of the submitted document. If the document type is not supported, then the document is not indexed.
  For more information about supported document types, refer to the topic *Searchable Content Types* in the Related Topics listed below.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Check the option selected for *Crawling Frequency*. If the *Crawling Frequency* is set to *Continuous crawling*, documents are picked immediately for indexing. If the *Crawling Frequency* is set to *Scheduled crawling*, indexing is executed only during the scheduled time period.
  For more information about *Crawling Frequency*, refer to the topic *Configuring Application Properties* in the Related Topics listed below.
- Check the Indexing failure listing to verify if the document is indexed successfully. If the document is displayed in this list, then you need to modify and re-submit it so that Platform Search uses the document for indexing.

  > **Note**
  >
  > You can modify the document by adding or deleting a field and then saving it again. This updates the document's timestamp in the BI platform repository and initiates the re-indexing of the document.

  For more information about documents that fail to be indexed, refer to the topic *Indexing failure listing* in the Related Topics listed below.
- Check the Adaptive Processing Server trace logs containing information about the indexing failure.
  1. Go to the **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\logging\` directory, containing the APS trace log with a .glf extension.
  2. Open the trace log file and search for the document SI_ID, that needs to be indexed.

     > **Note**
     >
     > You can find the document SI_ID from the document properties.

Unable to retrieve Crystal Reports documents

Platform Search indexes Crystal Reports content only for versions 2008, 2011, and 2013. It does not index content for Crystal Reports for Enterprise.

However, for Crystal Reports for Enterprise you can search for document metadata such as title, description, and keyword, which are document properties.

If the document contains indexable content, then you need to follow the same process as listed in the above mentioned section *Unable to retrieve search results from the newly added document containing the keyword.*

Unable to retrieve SAP BusinessObjects Explorer InfoSpaces

Check if SAP BusinessObjects Explorer servers are stopped or disabled. Enable the servers for Platform Search to retrieve the search results from SAP BusinessObjects Explorer.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The SAP NetWeaver Enterprise Search application is unable to retrieve results from the BI platform repository

- Check if Platform Search retrieves the search results using BI launch pad to find out if the problem is due to the Platform Search and SAP NetWeaver Enterprise Search integration.
- Check if OpenSearch is deployed correctly in the Web application server. The specific steps for validating the OpenSearch deployment depend on the type of Web application server in use.
- Check if the connector is created or configured correctly in the SAP NetWeaver Enterprise Search configuration. You need to use the correct connector for SAP NetWeaver Enterprise Search to federate results from Platform Search.
- Check if the communication is correct between the machines running SAP NetWeaver Enterprise Search and BI platform respectively. In case of any network issues in a distributed environment, SAP NetWeaver Enterprise Search may fail to federate the results.
- Check if SAP NetWeaver Enterprise Search user(s) are added to the BI platform with appropriate rights. To validate the user's rights, go to the *Authentication* area of the CMC and select *SAP*.

Related Information

Indexing Failure Listing [page 677]
Configuring Application Properties in the CMC [page 568]
Searchable Content Types [page 679]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23 Federation

23.1 Federation

Federation is a cross-site replication tool for working with multiple BI platform deployments in a global environment.

Content can be created and managed from one BI platform deployment and replicated to other BI platform deployments across geographical sites on a recurring schedule. You can complete both one-way replication and two-way replication jobs.

The benefits of Federation include the ability to:

- Reduce network traffic
- Create and manage content from a single site
- Increase performance for end users

When you replicate content using Federation, you can:

- Simplify administration needs for multiple deployments
- Provide a consistent rights policy across multiple offices for global organizations
- Obtain information faster and process reports at remote sites where data resides
- Save time by retrieving local and dispersed data faster
- Synchronize content from multiple deployments without writing custom code

Federation allows you to have separate security models, lifecycles, testing, and deployment times, as well as different business owners and administrators. For example, you can delegate administration features that restrict the sales application administrator from changing a human resources application.

You can replicate a variety of objects with Federation, as described in the following table.

Category	Object types you can replicate	Additional notes
Business Views	Business View Manager, DataConnection, LOVs, Data Foundation, and so on	All objects are supported, although not at the individual level.
Reports	Crystal reports, Web Intelligence, and Dashboard Design	Full client add-in and templates are supported.
Third-Party Objects	Excel, PDF, PowerPoint, Flash, Word, text, rich text, and Shockwave Flash files	
Users	users, groups, Inboxes, Favorites, and Personal Category	
Business Intelligence Platform	Folders, Events, Categories, Calendars, Access Levels, Hyperlinks, Shortcuts, Programs, Profiles, Object Packages, Agnostic	

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Category	Object types you can replicate	Additional notes
Universe	Universe, Connections, and Universe Overload	

The following scenarios highlight two examples of how your organization can use Federation.

Scenario 1: Retail (centralized design)

ACME store wants to send a monthly sales report to the different store locations using the one-way replication method. The administrator at the origin site creates a report that administrators at each destination site replicate and run against that store's database.

> **Tip**
>
> Localized instances can be sent back to the origin site that maintain each object's replicated info. For example, it will apply the appropriate logo, database connection information, and so on.

Scenario 2: Remote Schedule (distributed access)

The data is at the origin site. Pending replication jobs are sent to the origin site to run. Completed replication jobs are then sent back to the destination sites for viewing. For example, the data for a report may not be available on the destination site, but the user can configure the reports to run on the origin site before the completed report is sent back to the destination site.

23.2 Federation terms

The following list of terms introduces words and phrases that relate to Federation and may assist with its navigation and use.

BI application	The logical grouping of related Business Intelligence (BI) content with a specific purpose and audience. A BI application is not an object. One BI platform deployment can host multiple BI applications, each of which can have a separate security model, lifecycle, testing and deployment timeline, as well as separate business owners and administrators.
Destination site	A BI platform system that pulls replicated BI platform content from an origin site.
Local	The local system where a user or administrator is connected. For example, the administrator of a destination site is considered “local” to the destination site.
Locally run completed instances	Instances that are processed on the destination site and then sent back to the origin site.
Multiple origin sites	More than one site can serve as an origin site. For example, multiple development centers generally have multiple origin sites. However, there can be only one origin site per replication.
One-way replication	Objects are replicated only in one direction: from the origin site to the destination site. Any updates made at a destination site remain at that destination site.
Origin site	The BI platform system where the content originates.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Remote	A system that is not local to a user. For example, the origin site is considered “remote” to users and administrators of the destination site.
Remote connection	An object that contains information used to connect to a BI platform deployment, including username and password, CMS name, WebService URI and clean-up options.
Remote scheduling	Schedule requests that are sent from the destination site to the origin site. Reports on destination sites can be scheduled remotely, which sends the report instance back to the origin site for processing. Then the completed instance is returned to the destination site.
Replication	The process of copying content from one BI platform system to another.
Replication job	An object that contains information about replication scheduling, which content to replicate, and any special conditions that should be performed when replicating content.
Replication list	A list of the objects to be replicated. A replication list refers to other content such as users, groups, reports, and so on, in the BI platform deployment to be replicated together.
Replication object	An object that is replicated from an origin site to a destination site. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon.
Replication package	Created during the transfer, the replication package contains objects from a replication job. It can contain all the objects defined in the replication list, as in the case of a rapidly changing environment or initial replication. Or it can contain a subset of the replication list if the objects change infrequently compared to the schedule of the replication job. The replication package is implemented as a BI Application Resource (BIAR) file.
Replication refresh	All objects in a replication list are refreshed regardless of the last modified version.
Two-way replication	Acts the same as one-way replication, but two-way replication also sends changes in both directions. Updates to the origin site are replicated to each destination site. Updates and new objects on a destination site are sent to the origin site.

23.3 Managing security rights

Federation replicates content between separate deployments and requires collaboration with other administrators, therefore it is necessary to understand security before you begin using Federation.

Administrators in separate deployments must coordinate with each other before enabling Federation. After content is replicated, administrators can change content.

Specific rights on the origin and destination deployments are required to accomplish certain tasks:

- Rights required on the origin site
- Rights required on the destination site
- Rights required on Federation-specific objects
- Federation scenarios

➔ Tip

It is recommended that you read this chapter prior to enabling Federation.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.3.1 Rights required on the origin site

This section describes the actions on the origin site and the required rights of the user account connecting to the origin site. This is the account you enter in the remote connection object on the destination site.

Action	Description	Rights required
One-way replication	Performs replication only from the origin site to the destination site. **Note** "View" and "Replicate" rights are required on all objects being replicated, including objects that are automatically replicated by dependency calculations.	• "View" and "Replicate" rights on all objects you want to replicate • "View" right on the replication list
Two-way replication	Performs replication from the origin site to the destination site, and from the destination site to the origin site.	• "View" and "Replicate" rights on all objects you want to replicate • "View" right on the replication list • "Modify Rights" right on user objects to replicate any password changes
Scheduling	Allows remote scheduling to occur on the origin site from the destination site.	• "Schedule" right for all objects that you want to remotely schedule

Related Information

Rights required on the destination site [page 693]

23.3.2 Rights required on the destination site

This section describes actions applied to the destination site and the required rights of the user account that is running the replication job. This is the account of the user who created the replication job.

Note

Like other schedulable objects, you can schedule the replication job on behalf of someone else.

Action	Description	Rights required
All objects	Replicates objects regardless of one-way or two-way replication.	• "View", "Add", "Edit", and "Modify Rights" rights on all objects • "Modify User Password" right, for all user objects

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Action	Description	Rights required
First replication	The first time the replication job is run, no objects exist on the destination site yet. Therefore, the user account that the replication job is running under must have rights for all top-level folders and objects that will have content added to them.	• "View", "Add", "Edit", and "Modify Rights" rights on all top-level folders and default objects

Related Information

Rights required on the origin site [page 693]

23.3.3 Federation-specific rights

This section details scenarios that are specific to Federation.

Action	Description	Rights required
Object cleanup	Object cleanup deletes objects on the destination site.	• The account that the replication job is running under requires "Delete" rights on all objects that may be potentially deleted.
Disable cleanup for certain objects	When certain objects are replicated from the origin site, you may not want to delete them from the destination site if they are deleted on the origin site. You can safeguard this through rights. For instance, choose this option when users on the destination site start are using an object independently of users on the origin site. For example, in a replicated universe where users on the destination site create their own local reports using this universe, you may not want to lose the universe on the destination site if it is deleted from the origin site.	• Deny "Delete" rights of the user account the replication job is running under on the objects you want to keep.
Two-way replication with no modifications on the origin site	In certain circumstances you may choose two-way replication but do not want some objects on the origin site modified, even if they are changed on	• Deny "Edit" rights of the user account used to connect in the remote connection object.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Action	Description	Rights required
	the destination site. Reasons for this include: if the object is special and should only be changed by users on the origin site; or if you want to enable remote scheduling but do not want changes propagated back. **Note** For remote scheduling, you can create a job that only handles objects for remote scheduling. However, in this case ancestor objects are still replicated, including the report, the folder containing the report, and the parent folder of that folder. Any changes made on the destination site are replicated to the origin site, and changes made on the origin site are replicated to the destination site.	

23.3.4 Replicating security on an object

To keep security rights for an object, you must replicate both the object and its user or group at the same time. If not, they must already exist on the site you are replicating to and have identical unique identifiers (CUIDs) on each site.

If an object is replicated and the user or group is not replicated, or does not already exist on the site you are replicating to, their rights will be dropped.

Example

Group A and Group B have rights assigned on Object A. Group A has “View” rights and Group B has “Deny View” rights. If the replication job replicates only Group A and Object A, then on the destination site, Object A will have only the “View” rights for Group A associated with it.

When you replicate an object, there is a potential security risk if you do not replicate all groups with explicit rights on the object. The previous example highlights a potential risk. If User A belongs to both Group A and Group B, the user will not have permission to view Object A on the origin site. However, User A will be replicated to the destination site because he belongs to both groups. Once there, because Group B was not replicated, User A will have the right to view Object A on the destination site, but cannot view Object A on the origin site.

Objects that reference other objects that are not included in a replication job, or those not already on the destination site, are displayed in a log file. The log file shows that the object referenced the unreplicated object and dropped its reference.

Security on an object for a particular user or group is replicated only from the origin site to the destination site. You can set security on replicated objects on the destination site, but those settings will not be replicated to the origin site.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.3.5 Replicating security using access levels

To persist, rights must be defined by access levels. The object, user or group, and access level must be replicated at the same time, or they must already exist on the site you are replicating to.

Objects that assign explicit rights to a user or group that are not included in the replication job, or not already on the destination site, are displayed in its log file, which shows the object had rights assigned that were not replicated and those rights were dropped.

In addition, you can choose to automatically replicate “Access Levels” that are used on an imported object. This option is available on the replication list.

> **Note**
>
> Default access levels are not replicated, but references are maintained.

23.4 Replication types and mode options

Depending on your selection of replication type and replication mode, you may create one of four different replication job options:

- One-way replication
- Two-way replication
- Refresh from origin
- Refresh from destination

23.4.1 One-way replication

With one-way replication, you can replicate content in only one direction, from the origin site to a destination site. Any changes you make to objects on the origin site in the replication list are sent to the destination site. However, changes you make to objects on a destination site are not sent back to the origin site.

One-way replication is ideal for deployments with one central BI platform deployment where objects are created, modified, and administered. Other deployments use the content of the central deployment.

To create one-way replication, select the following options:

- Replication type = One-way replication
- Replication mode = Normal replication

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.4.2 Two-way replication

With two-way replication, you can replicate content in both directions between the origin and destination sites. Any changes made to objects on the origin site are replicated to destination sites, and changes made on a destination site are replicated to the origin site.

> **Note**
>
> To perform remote scheduling and to replicate locally run instances back to the origin site, you must select two-way replication mode.

If you have multiple BI platform deployments where content is created, modified, administered, and used at both locations, two-way replication is the most efficient option. It also helps synchronize the deployments.

To create two-way replication, select the following options:

- Replication Type = Two-way replication
- Replication Mode = Normal replication

Related Information

Remote scheduling and locally run instances [page 720]

23.4.3 Refresh from origin or refresh from destination

When you replicate content in one-way or two-way replication modes, the objects on the replication list are replicated to a destination site. However, not all of the objects may replicate each time the replication job runs.

Federation has an optimization engine designed to help finish your replication jobs faster. It uses a combination of the object's version and time stamp to determine if the object was modified since the last replication. This check is done on objects specifically selected in the replication list and any objects replicated during dependency checking.

However, in some cases the optimization engine may miss objects, which won't be replicated. In these cases, you can use “Refresh from Origin” and “Refresh from Destination” to force the replication job to replicate content, and their dependencies, regardless of the timestamps.

"Refresh from Origin" only sends content from the origin to the destination sites. "Refresh from Destination" only sends content from the destination sites to the origin site.

> **Example**
>
> The following three examples describe scenarios using “Refresh from Origin” and “Refresh from Destination” where certain objects will be missed due to the optimization.
>
> **Scenario 1:** The addition of objects that contain other objects into an area that is being replicated.
>
> Folder A is replicated from the origin site to the destination site. It now exists on both sites. A user moves or copies Folder B with Report B, into Folder A on the origin site. During the next replication, Federation will see

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

that Folder B's timestamp has changed and will replicate it to the destination site. However, Report B's timestamp does not change. Therefore, it will be missed by a regular one-way or two-way replication job.

To ensure Folder B's content is properly replicated, a replication job with “Refresh from Origin” should be used once. After this, the regular one-way or two-way replication job will replicate it properly. If this example is reversed and Folder B is moved or copied on the destination site, then use “Refresh from Destination”.

Scenario 2: The addition of new objects using LifeCycle Manager or the BIAR command line.

When you add objects to an area that is being replicated using LifeCycle Manager or BIAR command line, the object may not be picked up by a regular one-way or two-way replication job. This occurs because the internal clocks on the source and destination systems may be out of sync when using the LifeCycle Manager or BIAR command line.

> **Note**
>
> After importing new objects into an area that is being replicated on the origin site, it is recommended that you run a “Refresh from Origin” replication job. After importing new objects into an area that is being replicated on the destination site, it is recommended that you run a “Refresh from Destination” replication job.

Scenario 3: In between scheduled replication times.

If you add objects to an area that is being replicated and can't wait until the next scheduled replication time, you can use “Refresh from Origin” and “Refresh from Destination” replication jobs. By selecting the area where objects have been added, you can replicate content quickly.

> **Note**
>
> This scenario can be costly for large replication lists, so it is recommended that you do not use this option often. For example, it is not necessary to create replication jobs to refresh from the origin to destination mode on an hourly schedule. These modes should be used in “run now” or infrequent schedules.

> **Note**
>
> In some cases, you cannot use conflict resolution, including: “Refresh from Origin”: destination site option wins is blocked, or “Refresh from Destination”: origin wins option is blocked.

23.5 Replicating third-party users and groups

In Federation you can replicate third-party users and groups, specifically Active Directory (AD) and LDAP users and groups.

> **Tip**
>
> Read this section if you plan to replicate these types of users and groups or their personal content, such as favorite folders or Inboxes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Mapping users and groups

1. Map the users and groups on the origin site for Federation to replicate them properly.
2. Replicate the mapped users and groups to the destination site.

> **Note**
>
> Do not map groups and users separately on the destination site. If you do, they will have different unique identifiers (CUIDs) on the destination and origin sites, and Federation will not be able to match the user or groups.

> **Example**
>
> The administrator maps Group A with User A on the origin and destination sites. Both Group A and User A have different unique identifiers on the origin and destination sites. During replication, Federation cannot match them and Group A or User A are not replicated due to an alias conflict.

> **Note**
>
> Before replicating third-party users and groups, the destination site must be set up to use AD or LDAP authentication. However, you must also configure the destination site to use AD or LDAP so it can communicate to the directory server or domain controller.

> **Note**
>
> After replicating an AD or LDAP group for the first time, users in this group are unable to log on until the AD/LDAP Group Graph has been refreshed. This occurs automatically approximately every 15 minutes. To refresh AD/LDAP Group Graph manually, go to the *Authentication* page of the CMC, double-click *Windows AD* or *LDAP*, and then click *Update*.

> **Note**
>
> Be careful when replicating third-party groups. When you add new users to the group in the directory server, they will be able to log on to both sites. This security issue of AD or LDAP authentication is independent of Federation.
>
> If you log on to the destination and origin sites separately, or the group membership is updated on both sites using the update button on the CMC authentication page, a user account is created on both sites. The accounts will have different unique identifiers and Federation won't be able to replicate them properly.
>
> It is important to create the account on one site and then replicate it to the other.

23.6 Replicating universes and universe connections

When using Federation to replicate Universes between BI platform deployments, it is important to plan in advance. A Universe object cannot function without an underlying Universe Connection.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Universe Connection objects contain information required to connect to a reporting database. To function correctly, Universe Connection objects must contain valid information and allow a database connection to be established.

Note

If you are using two-way replication and replicate a Universe from the origin site to the destination site without its Universe Connection, in subsequent replications the origin site's Universe may have its relationship to the Universe Connection on the origin site overwritten or removed. To avoid this, always replicate the Universe Connections with the Universes.

To ensure that dependent Universe Connections are replicated with the Universes, always select the following options when you create or modify the replication list that contains the Universes:

- *Include connections used by selected universes*
- *Include universes required by selected universes*

Note

If a Universe's relationship with its Universe Connection has been overwritten or removed, open the Universe in Universe Designer, and under *File* > *Parameters*, modify the connection information.

The following two examples demonstrate the process of replicating Universes and their related Universe Connections.

Example

When replicating Universes and Universe Connections, you must ensure that the connectivity environment on the origin site matches the connectivity environment on the destination site.

For example, if the Universe Connection uses an ODBC connection called “TestODBC”, then there needs to be a correctly configured ODBC connection called “TestODBC” on the destination environment. The ODBC connection can resolve to the same database or to a different database. To ensure that Universes using this connection do not encounter connectivity issues, the schemas of the databases must be the same.

Example

If you want the replicated Universe on the destination site to use a different database than the Universe on the origin site uses, replicate the Universe Connection, but have the connectivity information on the destination site point to the desired database.

For example, if the Universe Connection on the origin site is using an ODBC connection called “Test” pointing to “DatabaseA”, make sure you have an ODBC connection on the destination site that is also called “Test” but pointing to “DatabaseB”.

23.7 Managing replication lists

Replication lists include content, such as users, groups, and reports in the BI platform deployment, that can be replicated together. Replication lists are accessed from the CMC.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Content types that can be replicated are explained in the following table.

Category	Supported objects
Repository objects	Objects that include Business Views, DataConnection, LOVs, Data Foundation, and more. **Note** All objects are supported, although not at the individual level.
Reports	Crystal reports, Web Intelligence documents, and Dashboards objects. **Note** Full Client Add-in and templates are supported.
Third-party objects	Excel, PDF, PowerPoint, Flash, Word, text files, rich text files, Shockwave Flash files.
Users	Users, groups, Inboxes, Favorites, personal Category.
Business Intelligence Platform	Folders, events, categories, calendars, custom roles, hyperlinks, shortcuts, programs, profiles, object packages, agnostic.
Universes	Universes, connections, universe overload.

Note

The following objects must be created on the origin site and then replicated to the destination site. If you create these objects on the destination site and then replicate them to the origin site, they will not function on the origin site.

- Business Views
- Business Elements
- Data Foundations
- Data Connections
- Lists of Values
- Universe Overloads

23.7.1 Creating replication lists

Replication lists are located in the Replication Lists area of the CMC. You can organize replication lists in folders and subfolders that you create.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.7.1.1 To create a replication list folder

1. Go to the *Replication Lists* area of the CMC.
2. Click *Replication Lists*.
3. Click *Manage* > *New* > *Folder*.
   The *Create Folder* dialog box appears.
4. Type a folder name and click *OK*.
   You can now create replication lists in this folder.

23.7.1.2 To create a replication list

1. Go to the *Replication Lists* area of the CMC.
2. Select the folder where you want to save your new replication list.
3. Click *Manage* > *New* > *New Replication List*.
   The *New Replication List* dialog box appears.
4. Type the title and description of the replication list.
5. For advanced options, click the *Replication List Properties* link.
   This allows you to specify which dependencies to automatically replicate from the origin site to the destination site.
6. Select the required options as described in the table.

Dependency object options	Definition
Include personal folders for selected users	Replicates a selected user's personal folders and their content.
Include personal categories for selected users	Replicates a selected user's personal categories.
Include universes for selected reports	Replicates any universe that selected report objects depend on.
Include members of selected user groups	Replicates users within a selected group.
Include universes required by selected universes	Replicates any universes that depend on other universes.
Include inboxes for selected users	Replicates a selected user's Inbox and its content.
Include user groups for selected universes	Replicates the user groups associated with a universe's overloads.
Include access levels set on selected objects	Replicates any access levels used on any of the selected objects.
Include documents for selected categories	Replicates any documents, including Word, Excel, and PDF, that are included in selected categories.
Include supported dependencies for selected Flash objects	Replicates any Crystal reports, hyperlinks, Web Intelligence documents or universes that the Flash object depends on.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Dependency object options	Definition
Include profiles for selected users and user groups	Replicates any profiles associated with selected users or groups.
Include connections used by selected universes	Replicates any universe connection objects used by selected objects.

> **Note**
>
> Some objects in the BI platform are dependent on other objects. For example, a Web Intelligence document is dependent on the underlying universe for its structure and content. If you replicate a Web Intelligence document but do not select the universe it uses, replication will not work on the destination site unless the universe was already replicated there. However, if you enable *Include universes for selected reports*, Federation automatically replicates the universes that the report depends on.

7. Click *Next*.
8. Select one or more objects to add to your replication list.
   - Use the arrow buttons to add or remove objects in the *Available Objects* folder.
   - Or, click *Repository objects* under *Replicate all* to replicate all Business View, Business Elements, Data Foundation, Data Connection, List of Values, and repository objects, including report images and functions.

> **Note**
>
> It is not possible to replicate top level folders located in the *Available Objects* folder.

9. Click *Save & Close*.

23.7.2 Modifying Replication Lists

After you create a replication list, you can modify its properties or objects.

23.7.2.1 To modify properties in a replication list

1. Go to the *Replication Lists* area of the CMC.
2. Select the *Replication List* you want to modify.
3. Click *Manage* > *Properties*.
   The *General Properties* dialog box appears.
4. Modify the title and description. You can also modify the other areas of the replication list while the *General Properties* dialog box is open.
5. If you want to modify dependency options, click *Replication List Properties* on the navigation list.
6. Click *Save & Close*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Creating replication lists [page 701]

23.7.2.2 To modify objects in a replication list

1. Go to the *Replication Lists* area of the CMC.
2. Select a *Replication List*.
3. Click *Actions* > *Manage Replication List*.
   The *Manage Replication List* dialog box appears with a list of objects included in the replication list.
4. Add or remove objects as desired.
5. Click *Save & Close*.

Related Information

Creating replication lists [page 701]

23.8 Managing remote connections

Remote connection objects contain the information needed to connect to a remote BI platform deployment.

> **Note**
>
> The remote connection object is created on a destination site BI platform deployment. The remote connection is the origin site.

You can view remote connections in the *Federation* area of the CMC.

23.8.1 Creating remote connections

A remote connection in Federation connects to a remote BI platform deployment. To establish a connection to the origin site where the content to be replicated is located, you must first create a remote connection on the destination site.

You can create folders and subfolders to organize your remote connections.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.8.1.1 To create a remote connection folder

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Click *Manage* > *New* > *Folder*.
   A *Create Folder* dialog box appears.
4. Type a folder name and click *OK*.
   You can now create remote connections in this folder.

23.8.1.2 To create a remote connection

To connect to a remote BI platform deployment, you must create a remote connection in Federation.

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Click *Manage* > *New* > *New Remote Connection*.
   The *New Remote System Connection* dialog box appears.
4. Enter a title, description, and related fields as required:

> **Note**
>
> All fields are mandatory, except "Description" and "Limit the number of cleanup objects".

Table 93:

Field	Description
Title	Name of the remote connection object.
Description	Description of the remote connection object. (Optional)
Remote System Web Service URI	URL to Federation Web Services, which is automatically deployed on your Java application server. You can use any Federation Web Services in the BI platform whether they are the origin or destination site, or another deployment. Use this format: **http://<application_yourserver_machine_name>:<port>/dswsbobje**. Example: **http://<mymachine.mydomain.com>:<8080>/dswsbobje**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Field	Description
Remote System CMS	The name of the CMS you want to connect to that is accessible through Federation Web Services. This will be treated as the CMS for the origin site. This is the format: **`CMS_Name:port`**. Example: **`<mymachine>:6400`** **Note** If you are using the default port 6400, specifying the port is optional.
User Name	The user name that is used to connect to the origin site. **Note** Ensure that the user name you are using has view rights on the replication list at the origin site deployment.
Password	The password of the user account to connect to the origin site.
Authentication	The type of account authentication to connect to the origin site. Options are: Enterprise, AD, or LDAP.
Cleanup Frequency (in hours)	How often replication jobs that use this remote connection object perform an object cleanup. Enter only positive whole numbers. The unit is hours. Default = 24.
Limit the number of cleanup objects to	The number of objects a replication job cleans up. (Optional)

5. Click *OK*.

Related Information

Managing object cleanup [page 711]

23.8.2 Modifying remote connections

After you create a remote connection, you can modify its properties and security options.

To modify a remote connection:

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Double-click the remote connection you want to modify.
   The *Remote Connection Properties* dialog box appears. You can modify the following properties:
   - *Title*
   - *Description*
   - *Remote System Web Service URI*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- *Remote System CMS*
- *User Name*
- *Password*
- *Authentication*
- *Cleanup Frequency (in hours)*
- *Limit the number of cleanup objects to*

4. Specify your changes.
5. Click *Save & Close*.

23.9 Managing replication jobs

A replication job is a type of object that runs on a schedule and is used to replicate content between two BI platform deployments in federation.

> **Note**
>
> Replicated objects on a destination site will be flagged with a replication icon as shown here: If there is a conflict, an object will be flagged with a conflict icon as shown here:

You can view a list of replication jobs in the *Remote Connection* folder in the *Federation* area of the CMC.

23.9.1 Creating replication jobs

A replication job is required to replicate content between two BI platform deployments in federation. Each replication job must have only one remote connection and one replication list associated with it.

23.9.1.1 To create a replication job

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections*.
3. Select a *Remote Connection* to contain the new replication job.

> **Caution**
>
> The CMC must be able to connect to Web Services in the remote connection URI to continue using the wizard.

4. Click *Manage* > *New* > *New Replication Job*.
   A *New Replication Job* dialog box appears.
5. Type a title and description of the replication job.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Click *Next*.
   A list of available replication lists on the origin site appears.
7. Select the *Replication List* you want to use with your replication job.
8. Click *Next*.
9. Select configuration options as described in the table below.

Option	Description
Enable object cleanup on destination	Forces the replication job to delete any replicated objects on the destination site, where the originating object on the origin site was removed. **Note** Object Cleanup will not delete objects replicated using dependencies or objects selected on the replication list.
One-way replication	Specifies that an object only replicates from the origin site to the destination site. Any changes made after replication to the object on the origin site are replicated to the destination site, but changes made on the destination site are not replicated back to the origin site.
Two-way replication	Specifies that objects are replicated in both directions; from the origin site to the destination site, and from the destination site to the origin site. Changes made to these objects after replication at one site are then automatically replicated to the other site.
Origin site takes precedence	Specifies that when a conflict is detected between an object on the origin site and its replicated version on the destination site, the version on the origin site takes priority.
No automatic conflict resolution	Specifies that no action is taken to resolve any detected conflicts.
Destination site takes precedence (Only available with two-way replication)	Specifies that when a conflict is detected between an object on the origin site and its replicated version on the destination site, that the version on the destination site takes priority.
Normal replication	Specifies that the replication job acts normally.
Refresh from origin	Replicates all content from the origin site to the destination site whether it has changed or not. You can replicate the entire replication list or only a portion of it.
Refresh from destination (Only available with two-way replication)	Replicates all content from the destination site to the origin site whether it has changed or not. You can replicate the entire replication list or only a portion of it.
Replicate all objects (Only visible with two-way replication)	Replicates the entire replication list. **Note** This is the most complete option but takes the longest to perform.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Description
Replicate remote schedules (Only visible with two-way replication)	Replicates pending remote instances from the destination site to the origin site, and forces completed instances from the origin site to the destination site.
Replicate document templates	Replicates all objects that aren't instances (locally run or reports that are checked for remote scheduling). This includes users, groups, folders, reports, and so on.
Replicate locally run completed instances	Replicates completed instances only from the destination site to the origin site.

10. Click *OK*.

Related Information

Managing object cleanup [page 711]
Managing conflict detection and resolution [page 713]
Remote scheduling and locally run instances [page 720]

23.9.2 Scheduling replication jobs

After you create a replication job, you can schedule it to run once or on a recurring basis. You can also schedule multiple replication jobs on one destination site from one origin site.

> **Note**
>
> If you schedule multiple replication jobs on one destination site, only one replication job can connect to the origin site at a time. All other replication jobs that try to connect will be moved to a pending state and remain pending until they are able to automatically connect to the origin site.

23.9.2.1 To schedule a replication job

1. Go to the *Federation* area of the CMC.
2. Select the *Replication Job* you want to schedule.
3. Click *Actions* > *Schedules*.
4. Select the desired scheduling options.

23.9.3 Modifying replication jobs

After you create a replication job in Federation, you can modify its properties.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.9.3.1 To modify a replication job

1. Go to the *Federation* area of the CMC.
2. Click *Remote Connections* folder.
3. Select the *Remote Connection* object that contains the *Replication Job* you want to modify.
4. Select the *Replication Job* you want to modify.
5. Click *Manage* > *Manage object properties*.
6. View and edit the *Properties*, *Schedule*, *History*, *Replication List*, and *User Security*, as necessary.

Sections	Description
Properties	Modify the name, description and other general properties and options of the replication job.
Schedule	Set the replication job to run on a recurring schedule.
History	View and administer all instances of the replication job.
Replication List	Change the selected replication list.
User Security	Set rights on the replication job.

23.9.4 Viewing a log after a replication job

Every time you run a replication job, Federation automatically produces a log file, which is created on the destination site. The log files use XML 1.1 standards and require a web browser that supports XML 1.1.

To view a replication log:

1. Go to the *Federation* area of the CMC.
2. Click *All Replication Jobs*.
3. Select a *Replication Job* from the list.
4. Click *Properties*.
   The replication job *Properties* page opens.
5. Click *History*.
6. Click the *Instance time* of the log file to view successful replication jobs, or click *Failed* status to view a log file of failed replication jobs.
7. Select desired instance to view the log file.
   The log file is generated in XML format and uses an XSL form to format the information into an HTML page.

   You can access the XML log from the computer that is running the Server Intelligence Agent that contains the Adaptive Job Server. You can find the log file at this location:

   - On Windows: **<InstallDir>**\SAP BusinessObjects XI 4.0\logging
   - On Unix: **<InstallDir>**/sap_bobj/logging

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.10 Managing object cleanup

In Federation, you should perform object cleanup throughout the lifecycle of your replication process, to make sure all objects that you delete from the origin site are also deleted from each destination site.

Object cleanup involves two elements: a remote connection and a replication job. A remote connection object defines general cleanup options, and a replication job performs the clean up when the appropriate interval passes.

23.10.1 How to use object cleanup

Separate replication jobs that use the same remote connection work together during object cleanup. This means that your replication job will clean up objects within its replication list, as well as objects within other replication lists that use the same remote connection. A remote connection is only considered the same if the parent of the replication job is the same remote connection object.

Example

Replication Jobs A and B replicate Object A and Object B. They both replicate from the same origin site and use the same remote connection. If the origin site deletes Object B , Replication Job A will see that Object B was deleted. Even though Replication Job B is the one replicating it, Object B will also be removed from the destination site. When Replication Job B executes it won't need to run an object cleanup.

Note

Only objects on the destination site are deleted during object cleanup. If you remove an object from the origin site that is part of a replication, the object will be removed from the destination site. However, if an object is removed from the destination site, it will not be removed from the origin site during object cleanup, even if the replication job is in two-way replication mode.

Objects that are deleted or removed from the replication list are not deleted from destination site. To properly remove an object that is specified in a replication list, you should delete it on both the destination site and the origin site. Objects that are replicated via dependency calculations are not deleted.

23.10.2 Object cleanup limits

In the remote connection object, you can define the number of objects a replication job will clean up at one time. Federation automatically tracks where the clean up job ends. This way, the next time you run a replication job, it starts the next clean up job at that point.

Tip

To complete a replication job faster, limit the number of objects for cleanup.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Example

Replication Jobs A and B are replicating Object A and Object B. Both objects are replicated from the same origin site and use the same remote connection.

If the origin site deletes Object B and the object limit is set to 1, the next time Replication Job A runs, it will only check if Object A has been deleted. This way, the Object B is not checked and will not be deleted.

Next, Replication Job B runs and starts the object cleanup at the point where Replication Job A ended. It will check if Object B has been deleted and remove it from the destination site. You can find this option on the remote connection object's property “Limit the number of clean up objects to:”

Note

If you do not select this option, all replication jobs that use this remote connection will check all objects for potential clean up.

23.10.3 Object cleanup frequency

You can set the how often a replication job performs object cleanup in the remote connection “Cleanup Frequency” field.

Note

You must enter a positive whole number, which represents the number of hours to wait between object cleanup processing.

Example

Replication Jobs A and B replicate Object A and Object B. Both objects are replicated from the same origin site and use the same remote connection.

If Object B is deleted from the origin site and all of the following conditions are true, the replication job will check if Object A has been deleted.

- The Object Limit is 1
- The cleanup frequency is 150 hours
- Replication Job A runs next

Because the object limit is 1, Object B will not be checked or deleted on the destination site.

The next cleanup occurs 150 hours after Replication Job A did the initial check. Although Replication Jobs A and B may execute many times before the 150 hour limit, neither will attempt to run an object cleanup. After 150 hours, the next replication job will execute and attempt cleanup. Then it will determine that Object B was deleted on the origin site, and then delete it on the destination site.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Enabling and disabling options

Each replication job can participate in object cleanup. Use “Enable Object Cleanup on destination” option on a replication job to instruct it whether to run an object cleanup. In some cases, you may have high priority replication jobs you do not want to participate in object cleanup, so you can execute them as quickly as possible. To do this, disable object cleanup.

Related Information

Object cleanup limits [page 711]

23.11 Managing conflict detection and resolution

In Federation, a conflict can occur when the properties of an object are changed on both the origin site and destination site. Both top level and nested properties of an object are checked for conflicts. For example, a conflict can occur if a report or the name of a report is modified on both the origin and destination sites.

Some instances do not create a conflict. For example, if the name of a report is modified on the origin site, and the description of the replicated version is modified on the destination site, the changes merge together and no conflict occurs.

23.11.1 One-way replication conflict resolution

In one-way replication, you have two choices for conflict resolution.

Origin site takes precedence

If a conflict occurs during one-way replication, the origin site object takes precedence. Any changes to objects on a destination site are overwritten by the origin site's information. For example, if a report is modified on both the origin site and the destination site, the destination site modification will be overwritten by the origin site version after the next replication job.

> **Note**
>
> Because the conflict is automatically resolved, it is not generated in the log file and does not appear in the conflicting object list.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

No automatic conflict resolution

If a conflict occurs and you select “No automatic conflict resolution”, the conflict is not resolved, a log file is not generated, and it does not appear in the conflicting object list.

Administrators can access a list of all replicated objects that are in conflict in the Federation area of the CMC. Objects in conflict are grouped together by the remote connection they used to connect to the origin site with. To access these lists, go to the Replication Errors folder in the Federation area of the CMC, and select the desired remote connection. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon. A warning message also appears in the *Properties* page.

> **Note**
>
> The list is updated when a replication job that uses a remote connection is completed. It contains all objects in conflict for all of the replication jobs that use its specific remote connection.

> **Note**
>
> Any user with access to the CMC and the replication job instances can access the XML log saved in the logfile directory. A destination site object's icon is flagged to indicate a conflict. During processing, a conflict log is created.

Abdul modifies Report A on the origin site. Maria modifies the replicated version on the destination site. The next time the replication job runs, the report will be in conflict as it has changed on both sites and it will not be resolved.

The destination report is maintained and changes to the origin's report are not replicated. Subsequent replication jobs will behave the same way until the conflict is resolved. Any changes on the origin site are not replicated until the conflict is manually resolved.

> **Note**
>
> In this case, the entire object is not replicated. Other changes that may not be in conflict are not brought over.

To manually resolve a conflict, you have three options:

1. Create a replication job that replicates only the objects in conflict. It must use the same remote connection object and replication list.
   To keep the origin site changes, create a replication job. Then set replication mode to “Refresh from Origin”, and set Automatic Conflict Resolution to “Origin site takes precedence”.
   To keep the destination site changes, create a replication job with Replication Type = “Two-way replication”, Replication Mode = “Refresh from Destination”, and Automatic Conflict Resolution = “Destination site takes precedence”

   > **Note**
   >
   > In replication mode, set “Refresh from Origin ” or “Refresh from Destination”, to select only the objects in conflict on the replication list. This way, other objects are not replicated. Next, schedule the replication job to run and it will replicate the selected objects and resolve the conflict as specified.

2. Create a replication job that replicates only the objects in conflict. It will need to use the same remote connection object. However unlike option 1, you may create a new replication list on the origin site. Use only the objects in conflict and create a new replication job which will use this focused replication list.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

To keep the origin site changes, set the Automatic Conflict Resolution to “Origin site takes precedence”. To keep the destination site changes, set Automatic Conflict Resolution to “Destination site takes precedence” and the Replication Type to “Two-way replication”.

3. For one-way replication jobs, you may only delete the object on the destination site. The next time the replication job executes, it replicates the object from the origin site to the destination site.

> **Note**
>
> Be careful when deleting an object because other objects that depend on it may be removed, stop working, or lose security. Options 1 and 2 are recommended.

23.11.2 Two-way replication conflict resolution

In two-way replication conflict, you have three choices for conflict detection:

- Origin site takes precedence
- Destination site takes precedence
- No automatic conflict resolution

Origin site takes precedence

If a conflict occurs, the origin site will take precedence and overwrite any changes to the destination site.

> **Example**
>
> Lily modifies the name of a report to Report A. Malik modifies the name of the replicated version on the destination site to Report B. After the next replication job runs, the replicated version on the destination site will revert to Report A.
>
> This will not generate a conflict in the log file, and it will not appear in the conflicting object list because the conflict was resolved according to the user's instructions on the origin site.

Destination site takes precedence

If a conflict occurs, the destination site keeps its changes and overwrites them to the origin site.

> **Example**
>
> Kamal modifies the name of a report to Report A. Peter modifies the name of the replicated version on the destination site to Report B. When the replication job runs, a conflict is detected. The name of the destination report remains as Report B.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

In two-way replication, changes are also sent back to the origin site. In this scenario, the origin site is updated and its report name is changed to Report B. This does not generate a conflict in the log file and it will not appear in the conflicting object list because the conflict was resolved according to the user's instructions.

No automatic conflict resolution

When “No automatic conflict resolution” is selected, a conflict will not be resolved. The conflict will be noted in a log file for the administrator, who can manually resolve it.

Note

An object's icon is flagged to indicate that a conflict exists.

Note

Although changes are replicated to both origin and destination sites in two-way replication, only the destination site's versions will be flagged with a conflict icon.

Note

Any user with access to the CMC and the replication job instances can access the XML log outputted in the logfile directory. A destination site object's icon is flagged to indicate a conflict. During processing, a conflict log is created.

The administrator can access a list of all replicated objects that are in conflict in the Federation area of the CMC. Objects in conflict are grouped together by the remote connection they used to connect to the origin site with. To access these lists, go to *CMC* > *Federation* > *Replication Errors* > *Remote Connection*.

Note

The list is updated when a replication job that uses a remote connection is completed. It contains all objects in conflict for all of the replication jobs that use its specific remote connection. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon.

Example

Michael modifies Report A on the origin site. Damien modifies the replicated version on the destination site. When the next replication job runs, the report is in conflict as it has changed on both sites and will not be resolved.

The destination report is kept and changes to the origin's report are not replicated. Subsequent replication jobs behave the same way until the conflict is resolved. Any changes on the origin site will not get replicated until the conflict is manually resolved by the administrator or delegated administrator.

Note

In this case, the entire object is not replicated. Other changes that are not in conflict are not replicated.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Any user with access to the CMC and the replication job instances can access the XML log outputted in the logfile directory. A destination site object's icon is flagged to indicate a conflict. During processing, a conflict log is created.

The administrator can access a list of all replicated objects that are in conflict in the Federation area of the CMC. Objects in conflict are grouped together by the remote connection they used to connect to the origin site with. To access these lists, go to *CMC* > *Federation* > *Replication Errors* > *Remote Connection*.

> **Note**
>
> The list is updated when a replication job that uses a remote connection is completed. It contains all objects in conflict for all of the replication jobs that use its specific remote connection. All replicated objects on a destination site will be flagged with a replication icon. If there is a conflict, objects will be flagged with a conflict icon.

To manually resolve a conflict, you have three options:

1. Create a replication job that replicates only the objects in conflict. It must use the same remote connection object and replication list.
   To keep the origin site changes, create a replication job. Then set the Replication Mode to "Refresh from Origin" and set Automatic Conflict Resolution to "Origin site takes precedence".
   To keep the destination site changes, create a replication job and set Replication Type to "Two-way replication", set Replication Mode to "Refresh from Destination", and set Automatic Conflict Resolution to "Destination site takes precedence".

   > **Note**
   >
   > In Replication Mode, set "Refresh from Origin" or "Refresh from Destination", to select only the objects in conflict on the replication list. This way, other objects are not replicated. Next, schedule the replication job to run and it will replicate the selected objects and resolve the conflict as specified.

2. Create a replication job that replicates only the objects in conflict. It will need to use the same remote connection object. However unlike option 1, you may create a new replication list on the origin site. Use only the objects in conflict and create a new replication job which will use this focused replication list.
   To keep the origin site changes, set the Automatic Conflict Resolution to: "Origin site takes precedence".
   To keep the destination site changes, set Automatic Conflict Resolution to: "Destination site takes precedence" and the Replication Type to: "Two-way replication".
3. Delete the object on the site you don't want it to be located.

> **Note**
>
> Be careful when deleting an object because other objects that depend on it may be removed, stop working, or lose security. Options 1 and 2 are recommended.

To keep the destination site changes, you can delete the object on the origin site. The next time the replication job executes, it replicates the object from the destination site to the origin site.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> Be careful when deleting a origin site's copy as other destination sites that replicate that object may execute their replication job before the copy has been replicated back. This will cause the other destination sites to delete their copy, which will be unavailable until the copy is returned.

To maintain the origin site changes, you can delete the object on the destination site.

23.12 Using Web Services in Federation

Federation uses Web Services to send objects and their changes between the origin and destination sites. Federation-specific web services are automatically installed and deployed in your BI platform installation. However, you may want to modify properties or customize deployments in Web Services to improve functionality, as described in this section.

> **Tip**
>
> To improve file management and functionality, enable file caching in Federation.

23.12.1 Session variables

If you are transferring a large number of content files in one replication job, you may want to increase the session timeout period of the Federation Web Services.

The property is located in the `dsws.properties` file:

<App Server Installation Directory>\dswsbobje\Web-INF\classes

For example:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\classes
```

To activate a session variable, enter:

session.timeout = x

Where “x ”is the desired time, “x” is measured in seconds. If not specified, the default value is 1200 seconds or 20 minutes.

The new properties take effect only after the modified web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.12.2 File caching

File caching allows Web Services to handle very large attachments without buffering them in memory. If it is not enabled during large transfer sizes, all of the Java's Virtual Machine memory can be utilized and replication may fail.

> **Note**
>
> File caching decreases performance as the Web Services process to files instead of memory. You may use a combination of both options and send large transfers to a file and smaller ones into memory.

To enable file caching, modify the `Axis2.xml` file located at:

<App Server Installation Directory>\dswsbobje\Web-Inf\conf

For example:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\conf
```

Enter the following:

```
<parameter name="cacheAttachments" locked="false">true</parameter>

<parameter name="attachmentDIR" locked="false">temp directory</parameter>

<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> **Note**
>
> Threshold size is measured in bytes.

The new properties take effect only after the modified web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

23.12.3 Custom deployment

Federation Web Services may deploy automatically and require the “federation”, “biplatform”, and “session” services to activate. To disable Federation or any other Web Services, modify the corresponding Web Services `service.xml` file.

BI platform Web Services are located in:

<App Server Installation Directory>\dswsbobje\WEB-INF\services

Example:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\services
```

To deactivate Web Services:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- add “activate” property in the service name tag of the `service.xml` file and set it to false
- restart your Java application server

For example, to disable Federation:

The `services.xml` file is located in:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\services\federator\META-INF
```

Change the service name from:

```
<service name="Federator">
```

To:

```
<service name="Federator" activate="false">
```

The new properties take effect only after the modified web application is redeployed on the computer running the web application server. Use WDeploy to redeploy the WAR file on the web application server. For information on using WDeploy, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

23.13 Remote scheduling and locally run instances

This section describes remote scheduling, locally run instances, and instance sharing. These features allow reports to run where the data resides and send completed instances to the appropriate locations.

23.13.1 Remote scheduling

Using Federation, you can schedule a report on the destination site and then process it on the origin site. The completed instance will be returned to the destination site.

To enable remote scheduling, schedule a report as normal and enable the option “Run at origin site”. To enable this option, click *Schedule* > *Scheduling Server Group* > *Run at origin site*. After the scheduled instances are created, they are placed in the pending stage.

During remote scheduling, information submitted on the destination site is disregarded and the report instance remains in the pending stage.

When the next replication job that manages the report is enabled for remote scheduling, it copies the instance to the origin site for processing. The instance remains in a pending state until the scheduler processes it. Meanwhile, the replication job that sent it will return any previously completed instances and object changes.

Once the instance has processed on the origin site, it reverts to a completed state. When the next replication job that manages the report is enabled for remote scheduling, it uses the completed instance to update the copy on the destination site. Once updated, the instance on the destination site is complete.

> **Note**
>
> A replication job has to run twice to bring back one completed instance.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Example

1. Tom schedules Report A for remote scheduling.
2. Report A is created on the destination site and is in the pending state.
3. Replication Job A runs. First, it replicates changes from the origin site to destination site (including previously completed instances). Second, it copies the instance in the pending state to the origin site, as well as changes to be replicated from the destination site to the origin site.
4. At the origin site, the scheduler picks up the instance in the pending state and sends it to the appropriate job server for processing. The instance is then processed and placed in the completed state on the origin site.
5. Replication Job A runs again. When it replicates content from the origin site to the destination site, the completed instance Report A is picked up and changes are applied to the destination's version.
6. Once this task is done, the destination's version is complete.

Remote scheduling only works with a two-way replication job. You must enable “Replicate remote schedules”. This option is located on the *Replication Job Properties* page in the “Replication Filters” area. In some scenarios, you may want to replicate remotely scheduled jobs more frequently than other objects on your replication list. To do this, create two replication jobs. Enable one job with “Replicate remote schedules” for a replication job that is only focusing on remote scheduling. Enable the other job with “Replicate document templates” or “Replicate all objects (no filter)”.

Note

When you enable remote scheduling, completed and failed instances appear on both the origin and destination site.

If a user on the destination site schedules a report for remote scheduling and the user does not exist on the origin site, the instance will fail on the origin site. The owner of the failed instance will be the user account of the remote connection object used to connect to the origin.

A replication job may only be configured for remote scheduling, but it always replicates the ancestor objects of the report instance. This means that if there are any changes between replications, it replicates the actual report, reports folder, and so on. If you do not want these changes on the destination site to be replicated to the origin site, you can use security rights to control which changes are replicated.

Related Information

Managing security rights [page 692]

23.13.2 Locally run instances

Locally run Instances are instances of a report that are processed from reports on the destination site. With Federation, you can replicate the completed instances from the destination site to the origin site.

To enable a replication job to replicate completed and failed instances from the destination site to the origin site, click *Replication Job Properties* > *Replication Filters* > *Replicate locally run completed instances*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

In some cases, you may want a replication job to only replicate locally run instances. To do this, enable “Replicate locally run completed instances”.

Note

When you enable locally run Instances on a replication job, both completed and failed instances are replicated to the origin site. This means that there will be copies on both the origin and destination sites.

Pending instances are never replicated.

If the owner of a locally run instance does not exist on the origin site, then the owner will be the user account used to connect in the remote connection object.

23.13.3 Instance share

When you enable Remote Scheduling and Locally Run Instances in a replication job, instance share may occur if one origin site with multiple destination sites are replicating the same report.

Example

Report A originates on the origin site, while destination sites A and B are replicating it. Instance share occurs at both destination sites:

- Enabled replication jobs with “Replicate remote schedules” and/or “Replicate locally run completed instances” Replicate Report A with the same replication job as above
- Schedule Report A on the destination site to “run at origin” and/or to run locally

If both destination sites A and B replicate Report A and their corresponding replication jobs are replicating remote schedules and/or replicating locally run instances, then any instances that were processed at destination site A and/or at the origin site on behalf of destination site A will be shared with destination site B.

Similarly, any instances processed at destination site B and/or processed at the origin site will also be shared with destination site A. Finally, the origin site and destination sites A and B will have an identical set of instances.

Instance share is ideal in many cases. For example, when users from other sites need to access information from their sister deployments. In this case, to prevent instances from being viewed by users at the local site, ensure the proper security rights are set. For example, in a report object, apply the rights so users can see only the instances they own.

Note

All objects follow the BI platform security rules. To ensure that users and groups can only view applicable instances, it is recommended that you set rights so that the users can only view instances that they own. For example, in a report object, apply the rights so users can see only the instances they own.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Managing security rights [page 692]

23.14 Importing and promoting replicated content

In some cases, you may choose to import or promote replicated content from one BI platform system to another. This section discusses these features in Federation.

> **Note**
>
> Object migrations are best performed by members of the Administrators group, in particular the Administrator user account. To migrate an object, many related objects may also need to be migrated. Obtaining the required security rights for all the objects may not be possible for a delegated administrator account.

23.14.1 Importing replicated content

If you use the LifeCycle Manager to import content from one BI platform deployment to another, the LifeCycle Manager does not import any of the replication-specific information associated with replicated objects that are being imported. This means that after the import, the object acts as if it was never replicated. This is specific to replicated objects on a destination site and is described in the following scenario.

> **Example**
>
> BI platform A is a destination site in a Federation process. Report A, a replicated report on System A, is imported from System A to BI platform B using the LifeCycle Manager.
>
> **Outcome:** When Report A is copied to BI platform B, it doesn't contain any replicated information. Report A will no longer be flagged with a replication icon. If the object was in conflict on BI platform A, it will not be in conflict on System B. Essentially it is treated as an object that originated from System B.
>
> > **Note**
> >
> > The CUID may or may not be the same, depending on the import choices you select in the LifeCycle Manager.

23.14.2 Importing replicated content and continuing replication

After you've imported replicated content, you may want to include the imported objects in a Federation process. There are two scenarios: treat the system that the imported objects reside on as an origin site, or treat the system as a destination site. To treat this system as an origin site, proceed with Federation as normal.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

To treat the system as a destination site and replicate the imported objects from the origin site, you must:

- Ensure the CUID of the objects are preserved when you use the LifeCycle Manager.
- Ensure the first replication job either has conflict resolution set to “Origin wins” or “Destination wins”.

Tip

Instead of importing the object using LifeCycle Manager from one destination site to another, it is more efficient and highly recommended to only use Federation to replicate the object.

Example

Report A was created on BI platform System A. System X used Federation to replicate Report A from System A to System X. The LifeCycle Manager then imported Report A from System X to System Y.

Plan: System Y wants to set up Federation to System A, and keep Report A as part of Replication. System Y is the destination and System A is the origin.

Action: When importing Report A from System X to System Y, the CUID of Report A must be preserved. In addition, when the first Replication Job executes, it will try to replicate Report A. Because the object already exists on System Y, replication will produce a conflict. To specify which version to use, you must set the Conflict Resolution mode to either “Origin wins” or “Destination wins”.

Note

In this example, it is recommended that instead of importing the object using LifeCycle Manager from one destination site to another, only use Federation to replicate the object. Report A will replicate from System A to System Y and it is unnecessary to use LifeCycle Manager to import from System X to System Y.

23.14.3 Promoting content from a test environment

In any organization, testing is often done before placing anything into a production environment. It is normal to test Federation between BI platform systems in a development or testing environment prior to setting Federation up on your production machines. Once you create your origin site and destination sites and content in a testing environment, you can promote this set up to your production machines using the following steps:

1. Use the LifeCycle Manager to promote your content from your origin site in the testing environment to the machine in production that will act as your origin site.

   Note

   The replication list object is not selectable when using the LifeCycle Manager.

2. Create the replication list on the origin site in the production environment and include the desired content.
3. Choose from these two following options:
   - A) Create a remote connection object and the appropriate replication jobs on the production machine(s) in production that will act as your destination site(s).
   - B) Use the LifeCycle Manager to import the remote connection and replication jobs from the destination site in Dev/QA to the production machines that will act as destination site(s). Then edit the imported remote connections to point to the machine in production that will act as the origin site.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

23.14.4 Re-pointing a destination site

Currently, after an object is replicated from an origin site, it must always be replicated from that origin site and cannot be replicated from another BI platform if the remote connection object is edited to point to a new system, any attempt to replicate an object that was replicated from a different BI platform system than the remote connection object will fail to replicate. To replicate an object from a different origin site, delete it from the destination site first.

> **Note**
>
> After you copy a replicated object, the CUID of the copy is changed and the copy will not contain any replication information.

23.15 Best practices

You can use Federation to optimize the performance of a replication job.

If there are a large number of objects in a single replication job, you can take additional steps to ensure that it runs successfully. Typically, you should be able to replicate up to 32,000 objects in each replication job. However, some deployments may require configurations with smaller or larger replication sizes.

1) Obtain a dedicated Web Services provider

In Federation, replicated content is sent using Web Services. In a default installation of the BI platform, all Web Services use the same web service provider. Larger replication jobs may utilize the web service provider longer and slow down its response to other web service requests as well as any applications it serves.

If you plan to replicate a large number of objects at once, or run several replication jobs in sequence, you may consider deploying Federation Web Services on its own Java Application server using your own web services provider.

To do this, use the BI platform installer to install web services. You must have a Java Application Server already running. If you do not, install the entire Web Tier Components option, which will install web services and Tomcat.

> **Note**
>
> You must provide information for an existing CMS (for example, host name, port, and administrator password).

> **Note**
>
> You will need to use this new Web Services provider's URI in your remote connection's URI field.

2) Increase the Java Application Server's available memory

Increase the available memory of your Java Application Server if your single replication job replicates many objects, or if you are sharing the Application Server with other applications.

If you deployed the BI platform and Tomcat, the default available memory is 1 GB. To increase the available memory for Tomcat:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

In Windows:

1. Click *Start* > *Programs* > *Tomcat* > *Tomcat Configuration*.
2. Select *Java*.
3. In the *Java Options* box, locate `-Xmx1024M`
4. Increase the `-Xmx1024M` to the desired size.

Example

To increase the memory to 2 GB, enter: `-Xmx2048M`

In Unix:

1. In the `<BOE_Install_Dir>/setup/`, open `env.sh` with your preferred text editor. Increase the `-Xmx1024m` parameter to the desired size.
2. Locate the following lines

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

3. Increase the `-Xmx1024m` parameter to the desired size.

Example

To increase the memory to 2 GB, enter: `-Xmx2048m`

Tip

For other Java application servers, refer to your Java application server's documentation to increase the available memory.

3) Reduce the size of the BIAR files being created.

Federation uses Web Services to replicate content between the origin site and destination site. Objects are grouped together and compressed into BIAR files for more efficient transportation.

When replicating a large number of objects, configure your Java Application Server to create smaller BIAR files. Federation will package and compress objects across multiple smaller BIAR files so the number of objects you want to replicate will not be limited.

To reduce the size of the BIAR files created, add the following Java parameters to your java application server:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

`bobj.biar.suggestSplit` suggests an appropriate size of the BIAR file, which it will try to meet. Suggested new value is 90MB.

`bobj.biar.forceSplit` will force a BIAR file to stop at a given size. Suggested new value is 100 MB.

> **Note**
>
> You do not need to change the default BIAR file size settings unless your application server is running out of memory and its maximum heap size cannot be increased any further.

For Tomcat Windows:

1. To open the *Tomcat Configuration* tool, click *Start* > *Programs* > *Tomcat* > *Tomcat Configuration*.
2. Select *Java*.
3. In the *Java Options* box, add the following lines at the end:

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

For Tomcat Unix/Linux:

1. Open the env.sh with your preferred text editor. It is located in `<BOE_Install_Dir>/setup/`
2. Locate the following lines:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120 -Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ]; then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Add the desired BIAR file size parameters.

Example: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

For other Java Application servers, consult your documentation to add Java system properties.

4) Increase the Socket Timeout.

The Adaptive Job Server is responsible for running the replication job. During the execution of the replication job, the Adaptive Job Server establishes a connection to the origin site. When receiving large amounts of information from the origin site, it is important that the Socket which the Adaptive Job Server is using to receive information does not timeout.

The default value is 90 minutes. You can increase the Socket Timeout if you need to.

To increase the Socket Timeout on the Adaptive Job Server:

1. Open the Central Management Console (CMC)
2. Navigate to the *Server* section and select *Adaptive Job Server*.
3. Click *Properties*.
4. Add “Command Line Parameters” to the end of the following:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- **Windows:** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>`
- **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>`

Related Information

Troubleshooting error messages [page 729]
Using Web Services in Federation [page 718]
Current release limitations [page 728]

23.15.1 Current release limitations

Federation is a flexible tool, however certain limitations may affect its performance during production. This section highlights areas that you can modify to optimize your Federation operations.

- Maximum number of objects
  Each replication job replicates objects between BI platform deployments. It is recommended that the maximum number of objects you replicate in a single replication job is 100,000. While a replication job may function with more than 100,000 objects, Federation only supports replicating up to 100,000 objects.
- Rights
  In Federation, rights are only replicated from the origin site to the destination site. It is recommended that user rights common to both deployments are set on the origin site and replicated to the destination sites using two-way replication. User rights on a specific site will be administered as usual in a BI platform deployment on the site where the user resides.
- Business Views and associated objects
  The BI platform may store Business Views, Business Elements, Data Foundations, Data Connections, and List of Values (LOVs). These objects are used to enhance the functionality of Crystal Reports.
  If these objects are first created on the destination site and then replicated to the origin site using two-way replication, they may not work properly and their data may not appear in Crystal Reports.
  It is recommended that you create the Business Views, Business Elements, Data Foundations, Data Connections, and LOVs on the origin site and then replicate them to the destination site. Make updates to the objects on the destination site or the origin site (rights permitting) and the changes will replicate back and forth properly.
- Universe overloads
  The BI platform may store universe overloads. If universe overloads are created on the destination site and then replicated to the origin site using two-way replication, they may not work properly.
  To resolve this, first create the universe overloads on the origin site and replicate them to the destination site. Second, set any security on the universe overloads on the origin site and replicate them to the destination site.
- Object cleanup
  Object cleanup deletes objects that have been deleted on the other site. Object cleanup is currently only done from the origin site to the destination site.
- Federation log files
  Federation log files are written to XML files that use XML 1.1 standards. To view the log files with a browser, the browser must support XML 1.1.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Managing object cleanup [page 711]

23.15.2 Troubleshooting error messages

This section contains error messages you may encounter in rare circumstances while using Federation. These messages will appear in the replication jobs logs or in the functionality area of a report.

1) Invalid GUID

Error example: `ERROR 2008-01-10T00:31:08.234Z The GUID ASXOOFyvy0FJnRcD0dZNTZg (found in property SI_PARENT_CUID on object number 1285) is not a valid GUID.`

This error means that you are replicating an object whose parent is not being replicated with it, and which does not already exist on the destination site. For example, an object is being replicated but not the folder that contains it. The parent object may not be replicated because the account replicating the objects does not have sufficient rights on the parent object.

2) Crystal Reports showing no data on the origin site

This error may occur if the Crystal report is using a Business View, Business Element, Data Foundation, Data Connection or List Of Values (LOVs) that was originally created on the destination site and then replicated to the origin site.

3) Universe overloads are not applied correctly

This error may occur if the report is using a universe which contains a universe overload that was created on the destination site and replicated to the origin site.

4) Java out of memory

Error example: `java.lang.OutOfMemoryError.`

This may occur if your Java Application Server has run out of memory while processing a replication job. Your replication job may be too big or your Java Application Server may not have enough memory.

Either increase the available memory of your Java Application Server by moving Federation Web Services to a dedicated machine, or reduce the amount of objects being replicated in one replication job.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

5) Socket timeout

Error example: `Error communicating with origin site. Read timed out.`

The information being sent from the origin site to the Adaptive Job Server on the destination site is longer than the allotted timeout. Increase the socket timeout on the Adaptive Job Server, or reduce the number of objects you are replicating in your replication job.

6) Query Limit

Error example: `SDK error occurred at the destination site. Not a valid query. (FWB 00025) …...Query string is larger than query length limit.`

This error may appear if you are replicating too many objects at one time and Federation submits a query that is too large for the CMS to handle. Objects from the origin site will be committed to the destination site. However, any changes that need to be committed to the origin site will not be committed. Conflicts are resolved as specified, however manual resolution conflict flags on the object will not be set. Objects committed on the destination site will continue to work properly.

To resolve this issue, reduce the number of objects you are replicating in one replication job.

7) Replication Job Times Out

Error example: `Object could not be scheduled within the specified time interval.`

You may receive this message if your replication job times out while it waits for another replication job to finish. This may occur if you have multiple replication jobs connecting to the same origin site at the same time. The failed replication job will try to run again at its next scheduled time.

To resolve this issue, schedule the failed replication job at a time that doesn't conflict with other replication jobs that connect to the same origin site.

8) Replication Limit

Error example: `SDK error occurred at the destination site. Database access error. …. Internal Query Processor Error: The query processor ran out of stack space during query optimization. Error executing query in ExecWithDeadlockHandling.`

You may receive this message if you exceed the number of supported objects that can be replicated at one time. To resolve this issue, reduce the number of objects you are replicating in your replication job and run the job again.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

9) Object dropped

Error example: `Error encountered while checking security rights`, or `Error encountered while packing object`.

This message may display if an object is dropped from the replication package. This can occur when Federation queries an object that needs replication, but before it checks for rights and the packs the object.

10) Adaptive Processing Server

Error example: `An error occurred in Job Processing Server`.

This error can occur when too many classes are loaded by Federation and there is not enough memory to process the replication job.

To resolve this issue, you need to perform both of the following steps:

1. In the command-line arguments of the Adaptive Processing Server, add the following line: `-javaArgs "XX:MaxPermSize=256m"`.
2. Add the following parameters to the Java Application server that you are connecting to for Federation, to reduce the size of the BIAR files that you are using:
   - `-Dbobj.biar.suggestSplit=100m`
   - `-Dbobj.biar.forceSplit=100m`

11) Object Manager Space

Error example: `Could not build push package. Input/Output exception occurred: "No space left on device."`

This occurs when the temporary directory that Federation uses doesn't have enough disk space. To resolve this issue, either create extra space in the temporary directory, or use a different location for the temporary directory.

To specify a different location for the temporary directory on the origin site, add the following line to the Java Application Server's configuration files: `-Dbobj.tmp.dir=`**`<TempDir>`**.

To specify a different location for the temporary directory on the destination site, add the following line to the Adaptive Processing Server's command-line arguments: `-javaArgs "-Dbobj.tmp.dir=`**`<TempDir>`**`"`.

In the above examples, **`<TempDir>`** is the location of the temporary directory that you want to use.

12) Universe Error

Error example: `An internal error occurred while calling processDPCommands API.`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This occurs when a Universe that has been replicated has an invalid or missing Universe-to-Universe Connection relationship. To resolve this issue, run the replication job with the *Refresh from Origin* option selected, and verify that they Universe Connection is replicated.

Alternatively, you can open the Universe in Universe Designer, edit the Universe's connection, and re-commit the Universe.

Related Information

Best practices [page 725]
Current release limitations [page 728]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24 Supplementary Configurations for ERP Environments

24.1 Configurations for SAP NetWeaver integration

24.1.1 Integrating with SAP Business Warehouse (BW)

24.1.1.1 Overview

This section shows how to configure BW to enable and administer report publishing from the SAP Business Warehouse application to the BI platform.

Before beginning this section, make sure you have completed the configuration of the SAP Authentication plugin in the CMC.

Related Information

Configuring SAP authentication [page 271]

24.1.1.1.1 Setting up folders and security in the BI platform

When you define an entitlement system in the BI platform, the system creates a logical folder structure to match your SAP system. When you import roles and publish content to the BI platform, corresponding folders are created. As an administrator, you do not have to create these folders. They are created as a consequence of defining an entitlement system when configuring the SAP authentication plugin, importing roles into the CMC, and publishing content to the BI platform.

> **Note**
>
> The BI platform administrator is responsible for assigning the correct rights to these folders:
>
> - *SAP top-level folder*
> Ensure the Everyone group has limited access to the SAP top-level folder.
> - *System ID folders*
> Assign the principal Publisher the following rights in the CMC:
>
> > **Note**
> >
> > The principal Publisher is not available until content is published.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Add objects to folder
- View objects
- Edit objects
- Modify the rights users have to objects
- Delete objects

Tip

To make rights administration easier, you can create a customized Publisher access level that includes these rights, and then grant the principal Publisher this access level on relevant System ID folders.

Related Information

Working with access levels [page 125]
How rights work in BI platform [page 112]

24.1.1.1.2 Understanding the default folder security patterns

When you publish content to the BI platform from SAP, the platform automatically creates the remaining hierarchy of roles, folders, and reports. The system organizes your reports in folders that are named according to the System ID and Client Number, and according to the name of the role:

- The system creates top-level folders—that is, the SAP, 2.0, and system (**<SID>**) folders—when you define an entitlement system.
- The system creates Role folders (imported as groups into the BI platform) as necessary, when a role is published from BW.
- The system creates a Content folder for each role that content is published to.
- Security is set on each report object, so users can view only the reports that belong to their roles.

The administrator is responsible for assigning rights to members of different roles. The Content Administration Workbench is used to administer report publishing functionality from within SAP BW. You can identify roles from the SAP BW system with particular BI platform systems, publish reports, and synchronize reports between SAP BW and a BI platform deployment.

Content folders

The BI platform imports a group for each role that is added to the entitlement system as defined in the CMC.

To ensure that suitable default rights are granted to all members of a content-bearing role, grant the appropriate rights in the Content Administration Workbench for each entitlement system that is defined in the BI platform. To start the Content Administration Workbench, run transaction /CRYSTAL/RPTADMIN:

1. In the Content Administration Workbench, expand *Enterprise system* and then expand *Available systems*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Double-click the system you want.
3. Click the *Layout* tab.
4. Set *Default security policy for reports* to *View*.
5. Set *Default security policy for role folders* to *View On Demand*.
6. Click *OK*.

These settings are reflected in the BI platform for all content roles. That is, roles that have content published to them. Members of these roles will now be able to view scheduled instances of reports published to other roles and will be able to refresh reports published to roles that they are a member of.

> **Note**
>
> It is strongly recommended that you keep the activities of roles distinct. For example, while it is possible to publish from an administrator role, it is better practice to publish only from publisher roles. Additionally, the function of publishing roles is only to define which users can publish content. Thus, publishing roles should not contain any content; publishers should publish to content bearing roles that are accessible to regular role members.

24.1.1.2 Configuring the BW Publisher

The BW Publisher allows you to publish Crystal reports (.rpt files) individually or in batches from BW to the BI platform.

On Windows, you can configure the BW Publisher in one of two ways:

- Start the BW Publisher using a service on a machine hosting the BI platform. The BW Publisher service will start instances of the BW Publisher as required.
- Start the BW Publisher using a local SAP Gateway to create BW Publisher instances.

You must select the configuration method based on the requirements of your site, after considering the advantages and disadvantages of each configuration. Once you have configured the BW Publisher in the BI platform, you must configure publishing in the Content Administration Workbench.

24.1.1.3 Configuring the BW Publisher as a service

This section explains how to enable publishing of reports from BW to the BI platform using the BW Publisher as a service, perform the following procedure.

24.1.1.3.1 Distributing the BW Publisher installation

This section explains the distribution of BW Publisher service and how to separate the BW Publisher from other BI platform components.

You can load-balance publishing from BW by installing BW Publisher services on two separate machines in the same BI platform system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

When you install the BW Publisher on the machines hosting the BI platform, configure each one to use the same Program ID and SAP Gateway Host and Gateway Service. After you create an RFC destination that uses this Program ID, BW load-balances publishing between the machines hosting the BI platform. Moreover, if one BW Publisher becomes unavailable, BW continues to use the remaining BW Publisher.

You can add an additional level of system redundancy to any configuration that includes multiple BW application servers. Configure each BW application server to run an SAP Gateway. For each one, install a separate BW Publisher service on a machine hosting the BI platform. Configure each BW Publisher service to use the Gateway Host and Gateway service of a separate BW application server. In this configuration, publishing from BW can continue if either a BW Publisher or an application server fails.

If you want to separate the BW Publisher from other BI platform components, install the BW using a stand-alone SAP Gateway.

In this case you must install a local SAP Gateway on the same machine as the BW Publisher. In addition, the BW Publisher requires access to the BI platform SDK and the SAP Crystal Reports Print Engine. Thus, if you install the BW Publisher and the local SAP Gateway on a dedicated machine, you must also install the SIA Server.

24.1.1.3.2 Starting the BW Publisher: UNIX

Run the BW Publisher script to create a publisher instance or instances to handle publishing requests. It is recommended that you start one publisher instance.

Once the BW Publisher starts, it establishes a connection with the SAP Gateway Service that you specified when you ran the BI platform installation program.

24.1.1.3.3 Starting the BW Publisher: Windows

On Windows, use the Central Configuration Manager™ (CCM) to start the BW Publisher service. When you start the BW Publisher service it creates a publisher instance to service publishing requests from your BW system. If the volume of publishing requests increases, the BW Publisher automatically spawns additional publishers to meet the demand.

24.1.1.3.4 Configuring a destination for the BW Publisher service

To enable the BW Publisher, you must configure an RFC destination on your BW server to communicate with the BW Publisher service. If you have a BW cluster, configure the RFC destination on each server, using the central instance of BW as your Gateway Host in every case.

If you want to publish to multiple BI platform systems from BW, create a separate RFC destination for the BW Publisher service in each BI platform deployment. You must use unique Program IDs for each destination, but the same Gateway host and Gateway service.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.3.5 Configuring the BW Publisher with a local SAP Gateway

> **Note**
>
> Do not use this configuration if the BI platform is installed on UNIX. Using this method on UNIX could result in unpredictable system behavior.

To enable publishing of reports from BW to the BI platform, using a local SAP Gateway, perform the following procedure:

- Installing a local SAP Gateway [page 737].
- Configuring a destination for the BW Publisher [page 737].

24.1.1.3.6 Installing a local SAP Gateway

A local SAP Gateway must be installed on the machine where you installed the BW Publisher. It is recommended that an SAP BASIS administrator perform the installation of one of these SAP Gateways.

For up-to-date instructions on installing a local SAP Gateway, see the SAP installation instructions included on your SAP Presentation CD.

For a detailed list of tested environments, consult the Product Availability Matrix (PAM) at http://service.sap.com/pam. The PAM includes specific version and Service Pack requirements for application servers, operating systems, SAP components, and so on.

After you have installed the SAP Gateway, use `regedit` to verify the `TMP` and `TEMP` registry entries under the `HKEY_CURRENT_USER\Environment` subkey. Both registry entries should hold the same string value, which must be a valid absolute directory path. If either entry's value contains the `%USERPROFILE%` variable, replace it with an absolute directory path. Typically, both registry entries are set to `C:\WINDOWS\TEMP`

24.1.1.4 Configuring a destination for the BW Publisher

To enable the BW Publisher, you must configure an RFC destination to provide BW with the location of the machine where you have installed the local SAP Gateway and the BW Publisher.

24.1.1.5 Configuring publishing in the Content Administration Workbench

The Content Administration Workbench is used to administer report publishing functionality from within SAP BW. You can identify roles from the SAP BW system with particular BI platform systems, publish reports, and synchronize reports between SAP BW and a BI platform deployment. Once you have set up SAP authentication,

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

and have configured the BW Publisher, perform the functions outlined in this section to enable publishing. These instructions will allow you to:

- Set appropriate authorizations for different users of the Content Administration Workbench.
- Set up connections to the BI platform where content is published.
- Define which roles can publish to each BI platform.
- Publish content from BW to the BI platform.

24.1.1.6 Users who can access the Content Administration Workbench

There are three types of users who may access the Content Administration Workbench:

- Content consumers, who belong to content-bearing roles and who can view reports. They do not have authorization to do anything other than view reports.
- BI platform content publishers, who can view, publish, modify, and (optionally) delete reports from BW.
- BI platform administrators, who are able to perform all tasks within Content Administration Workbench. These tasks include defining BI platform systems, publishing reports, and performing report maintenance.

24.1.1.7 Creating roles in BW for designated content publishers

When you are configuring BW for integration with the BI platform, assess whether or not your current role structure allows you to quickly designate particular BW users as content publishers or system administrators for the BI platform systems.

It is suggested that you label any new roles you create in a descriptive manner. Examples of descriptive role names would include `BOE_CONTENT_PUBLISHERS` and `SBOP_SYSTEM_ADMINISTRATORS`.

> **Tip**
>
> You can assign an administrative user either full system administration rights or a subset of those rights.

To modify the rights that these new roles (or any of your existing roles) are granted in the BI platform, you must first set up SAP Authentication and import the roles. You can then modify the rights of each imported role using the Central Management Console.

For details on creating roles, see your SAP documentation. For more information on the use of roles in administering content, see the following sections:

- Importing SAP roles [page 278].
- Setting up folders and security in the BI platform [page 733].
- Understanding the default folder security patterns [page 734].

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.8 Configuring access to the Content Administration Workbench

For each type of user that can access the Content Administration Workbench, you must apply the appropriate set of authorizations within BW. The authorizations are listed in the following tables.

Table 94: Authorizations for administrative users

Authorization object	Field	Values
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Change, Display (02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Create new, Change, Display, Delete (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Create new, Delete (01, 06)
ZCNTADMRPT	ACTVT	Display, Delete, Activate, Maintain, Check (03, 06, 07, 23, 39)

Table 95: Authorizations for content publishers

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Values
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Display (03)
ZCNTADMJOB	ACTVT	(New, Delete) 01, 06
ZCNTADMRPT	ACTVT	Display, Activate, Maintain, Check (03, 07, 23, 39) Delete (optional) (06) Edit (optional) (02)

Granting content publishers the right to delete reports in the BW Content Administration Workbench is optional. However, be aware that deleting a report in BW also deletes the report in the BI platform. If publishers do not have sufficient rights to delete reports in the platform, an error results.

Authorizations for content consumers

Table 96:

Authorization object	Field	Values	
S_RFC	RFC_TYPE	FUGR	
	RFC_NAME	SH3A, SUNI	
	ACTVT	Execute (16)	
		TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Execute (16)	
	RSADMWBOBJ	WORKBENCH	
		ACTVT	Display (03)

24.1.1.9 Defining a BI platform system

You must create a system definition within the Content Administration Workbench for each BI platform system to which you want to publish reports.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.9.1 To add a BI platform system

1. Execute the transaction `/crystal/rptadmin` to access the Content Administration Workbench.
2. From the *Operations* pane, select *Enterprise System*.
3. Double-click *Add new system*.
4. On the *System* tab:
   - Type a descriptive name in the *Alias* field. Avoid using spaces or special characters, as these characters need special treatment when the alias name is used while configuring Enterprise Portals.
   - Type the name of the machine that is running your CMS. If you configured your CMS to listen on a port other than the default, type **`CMSNAME:PORT`**.
   - Select *Default system* if you want to publish reports to this system from any role that has not been explicitly assigned to a BI platform system. Only one BI platform system can be the default.
     In the list of all available systems, the default system is indicated with a green checkmark.
5. Click *Save*.
6. On the *RFC Destinations* tab, add each RFC destination that is associated with this system.

   To add a destination, click the *Insert Row* button. In the list that appears, double-click the name of the RFC destination.

   > **Note**
   >
   > A BI platform system may have multiple destinations to add system redundancy. See "Distributing the BW Publisher installation".

7. Select the check box beside the destination name you added, and click *Verify BOE definition*.

   This test verifies that BW can contact the specified BW Publisher, and can log on to this system using the Crystal entitlement user account.
8. On the *HTTP* tab:
   - In the *Protocol* field, type **`http`** or **`https`**, if the web server that is connected to the BI platform is configured for HTTPS.
   - In the *Web server host and port* field, type the fully qualified domain name or IP address of the web server that hosts BI launch pad. For an installation that uses a Java application server, include the port number. For example, type **`boserver01.businessobjects.com:8080`**.
   - In the *Path* field, type **`SAP`**
     This path is essentially the virtual path that your web server uses when referring to the `sap` subfolder of your BI platform web content. Provide an alternate value only if you have customized your web environment and the location of the platform web content files.
     Do not include a forward slash at the beginning or at the end of this entry.
   - In the *Viewer application* field, type the name of your viewer application.
     To use the default BI platform viewer that uses the Java version of BI launch pad, type **`openDocument.jsp`**
     If the BI platform was installed on Windows using the default `ASP.NET` configuration, to use the default browser, type **`report/report_view.aspx`**
9. On the *Languages* tab, select the languages of reports that will be published to this system.
10. On the *Roles* tab, add the content-bearing roles that you want to associate with this BI platform system.

    See "Importing SAP roles".

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

11. Click the *Insert Row* button.

    A list of roles available to add to this system appears.

    > **Note**
    >
    > Each role can publish to only one BI platform system. If the roles you want to add to this BI platform system do not appear in the list, click *Cancel* to return to the *Roles* tab, and click *Reassign Roles*.

12. Select the roles you want to publish to this system and click *OK*.
13. On the *Layout* tab, select the default security settings for reports and roles folders published to this BI platform system.

    > **Note**
    >
    > A folder is created automatically in the BI platform for each role published to that system. The folder contains shortcuts to the reports published under that role.

    > **Note**
    >
    > Once you have configured a BI platform system, changing the default security levels here will not affect the security levels of published role folders or reports. To change the default security levels for all roles and content published to the platform, delete the roles folders and shortcuts in the system. (This will not delete the actual reports.) Change the security settings here, and republish the roles and reports.

14. Click *OK* at the bottom to save your settings and to create the BI platform system in the Content Administration Workbench.

You are now able to publish reports to the BI platform from BW.

Related Information

Distributing the BW Publisher installation [page 735]
Importing SAP roles [page 278]

24.1.1.10 Publishing reports using the Content Administration Workbench

After a report has been saved to BW, you can publish it using the Content Administration Workbench. You can use the Content Administration Workbench to publish individual reports, or you can publish all reports saved to a particular role. Only a user who has the authorizations granted to a Crystal content publisher (see Creating and applying authorizations [page 757]) can use the Content Administration Workbench to publish and maintain reports.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.11 Publishing roles or reports

1. Execute the transaction `/crystal/rptadmin` to access the Content Administration Workbench.
2. From the *Operations* pane, select *Publish reports*.
3. To find content saved to your BW system, double-click *Select reports and roles to publish*.
   A dialog box designed to help you filter the available roles and reports appears.
4. From the list, select the system or systems containing content that you want to display.

   > **Note**
   >
   > The list contains all available systems defined on the BW system.

5. Next, filter your results to limit the number of reports and roles that will be displayed. Use these options:
   - *Object version*
     Selecting "A: active" displays all reports that can be published. Selecting the blank option displays all reports. (The remaining options are SAP reserved terms.)
   - *Object status*
     Select "ACT Active, executable" to display only reports that have been published. Select "INA Inactive, not executable" to display only reports which have not been published. Leave the field blank to display all reports. (The remaining options are SAP reserved terms.)
   - *Role filter*
     If you type text in this box, only the roles that match what you type here are displayed. Use * as a wildcard character. For example, to display all roles beginning with the letter d, type "d*".
   - *Report description*
     If you type text in this box, only the reports whose descriptions match what you type here are displayed. Use * as a wildcard character to match any number of characters. Use + as a wildcard to match 0 or 1 characters. For example, to display all reports whose description contains the word revenue, type *revenue*.
6. Click *OK*.
   The list of reports that meet your criteria appears in the right-hand panel.
   The reports are arranged in a hierarchy: BI platform system > Roles on that system > Reports saved to the role.
   Each item in the hierarchy is labeled with a red, yellow, or green dot. Items higher in the hierarchy reflect the status of the items that they contain, with the least favorable condition percolated to the top of the hierarchy. For example, if one report in a role is yellow (active), but all of the rest are green (published), then the role shows as yellow (active).
   - Green: The item is fully published. If the item is a BI platform system or a role, all reports in that item are published.
   - Yellow: The item is active, but not published. If the item is a report, the item is available for publishing. If the item is a role or a BI platform system, then all content is active and at least one item that the role or system contains has not been published.
   - Red: The item is SAP content, and is not available for publishing using the Content Administration Workbench. Content is not available for publishing until it has been activated using the BW Administration Workbench.
7. Select the reports that you want to publish.
   To publish all of the reports in a role, select the role. To publish all roles on a BI platform system, select the system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> When you select a role (or a system), all reports contained in that role (or system) are selected. To clear this selection, clear the role (or system) check box, and then click Refresh.

8. Click *Publish*.

> **Note**
>
> Reports published in the background are processed as system resources become available. To use this option, click *In background* instead of *Publish*.

9. Click *Refresh* to update the display of the status of BI platform systems, roles, and reports in the Content Administration Workbench.

> **Tip**
>
> To view a report, right-click the report and select *View*. To see which queries are used by the report, right-click the report and select *Used Queries*.

> **Note**
>
> After you have published a report to the BI platform, if you want to overwrite the report you published, click *Overwrite*.

Related Information

Scheduling background publishing [page 744]

24.1.1.12 Scheduling background publishing

Publishing reports in the background, either immediately or as a scheduled job, conserves system resources. It is recommended that you publish reports in the background to improve system responsiveness.

Publishing reports periodically, as scheduled jobs, synchronizes the report information between BW and your BI platform deployment. It is recommended that you schedule all reports (or roles containing these reports). You can also manually synchronize roles and reports using the Update status option of the Report Maintenance operation. See Updating the status of reports [page 745] for details.

24.1.1.13 Updating system information for published reports

The BW Publisher uses the SAP system information entered here to update the data source of published reports. You can choose to use the local BW application server, or the central BW instance if you prefer a load balancing configuration.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.14 Maintaining reports

Report maintenance tasks include synchronizing information about reports between the BI platform and BW (Update status), deleting unwanted reports (Delete reports), and updating reports migrated from previous versions of the platform (Post-migration).

24.1.1.14.1 Updating the status of reports

If you make a change to a published report on a BI platform system (such as changing which role a report is published to), the change is not reflected in BW until you synchronize the BI platform and BW. You can schedule a publishing job to periodically synchronize the BI platform and BW (see Scheduling background publishing [page 744]), or you can manually update the status of the report using the Report Maintenance tool.

24.1.1.14.2 Deleting reports

Deleting a published report from BW using the Content Administration Workbench also deletes the report from the BI platform. Only users who have been granted the authorizations necessary to delete reports on both BW and the BI platform system can remove reports.

> **Note**
>
> If a user has rights to delete a report on BW, but not on the BI platform system where that report is published, you may encounter an error.

24.1.1.15 Configuring the SAP http request handler

To enable viewing of reports in BW, you must configure BW to use the http request handler that is included as part of the Content Administration Workbench. Then, when a BW user opens a Crystal report from within the SAPGUI, BW can route the viewing request over the Web appropriately.

Use the transaction SICF to access the list of virtual hosts and services active on your BW system. Create a new node named `ce_url` under BW in the `default_host` hierarchy and add `/CRYSTAL/CL_BW_HTTP_HANDLER` to the handler list. You may have to manually activate this service after creating it.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.16 Configurations for processing SAP data

24.1.1.16.1 Processing scheduled reports in SAP's batch mode

For Windows installations, you can run scheduled reports in the BI platform using SAP's batch mode. The InfoSet and Open SQL drivers can run reports using SAP's batch or background mode when specific environment variables are set to 1. The relevant environment variables are:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (for the InfoSet driver)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE` (for the Open SQL driver)

However, it is recommended that you use this feature only when you have a distributed installation of the BI platform. When these environment variables are set to 1, the drivers run reports using SAP's batch mode, regardless of the reporting component that is actually running the report. Therefore, if you create these environment variables as system environment variables on a machine that is running a combination of BI platform servers, the drivers run all reports in batch mode (including on-demand report requests from the Crystal Reports Processing Server and the Report Application Server).

To ensure that the drivers run only your scheduled reports in batch mode (reports run by the Adaptive Job Server), avoid setting system environment variables on machines running combinations of BI platform servers. Instead, follow these steps to customize the environment variables for each Adaptive Job Server.

> **Note**
>
> SAP users who schedule reports in the BI platform may require additional authorizations in SAP.

Related Information

Scheduling a report in batch mode using an Open SQL query [page 772]

24.1.1.16.2 To process scheduled reports in SAP's batch mode

1. Create a batch script (`.bat` file) in a text editor such as Notepad, with the following contents:

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
   %*
   ```

   This script sets the environment variables to 1 and then executes any parameters passed to the script from the command line.
2. Save the file as `jobserver_batchmode.bat` to a folder on each Adaptive Job Server machine.
3. Log on to the Central Management Console (CMC).
4. Choose *Servers*.
5. Expand the *Service Categories* node, and choose *Analysis Services*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

6. Select *Adaptive Processing Server*, and choose *Properties* in the context menu.
   The *Properties* page opens.
7. On the *Properties* page, locate the *Command line Parameters* field.

   This is the startup command for the Adaptive Job Server. For example:

   ```
   "\\SERVER01\C$\Program Files\SAO Business Objects\SAP BusinessObjects Enterprise
   \win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType
   BusinessObjects Enterprise.Report -lib procReport -restart
   ```
8. Precede the default command with the full path to the `jobserver_batchmode.bat` file that you saved on the Adaptive Job Server machine.

   In this example, the batch file is saved on a machine named SERVER01 as:

   ```
   C:\Crystal Scripts\jobserver_batchmode.bat
   ```

   The new startup command for the Adaptive Job Server is:

   ```
   "\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$\Program
   Files\SAP Business Objects\SAP
   BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name
   SERVER01.report  -ns SERVER01
   -objectType BusinessObjects Enterprise.Report -lib procReport  -restart
   ```

   This new startup command launches the batch file first. The batch file in turn sets the required environment variables before executing the original startup command for the Adaptive Job Server. This ensures that the environment variables available to the Adaptive Job Server differ from the environment variables available to servers responsible for on-demand reporting (the Crystal Reports Processing Server and Report Application Server).
9. Click *Save & Close*.
10. Right-click the Adaptive Job Server and select *Start* in the context menu.

> **Note**
>
> If the Adaptive Job Server fails to start, verify your new startup command.

24.1.1.17 Configurations for SAP transports

24.1.1.17.1 Overview

The BI platform includes these transports:

- Open SQL Connectivity transport
- InfoSet Connectivity transport
- Row-level Security Definition transport
- Cluster Definition transport
- Content Administration Workbench transport
- BW Query parameter personalization transport
- MDX transport

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- ODS transport

There are two different sets of the transports: Unicode compatible transports and ANSI transports. If you are running a BASIS system of 6.20 or later, use the Unicode compatible transports. If you are running a BASIS system earlier than 6.20, use the ANSI transports. All the installed transports are located in the following directory on your product distribution media: `\Collaterals\Add-Ons\SAP\Transports\`.

> **Note**
>
> When checking for possible installation conflicts, ensure that none of the object names already exists in your SAP system. Objects use a **`/crystal/`** namespace by default, so it is not necessary to create this namespace yourself. If you do create the **`/crystal/`** namespace manually, you will be prompted for license repair keys that you cannot access.

24.1.1.17.2 Configuring transports

To set up the Data Access or BW Publisher components of the BI platform , you must import the appropriate transports into your SAP system. These components use the contents of these transport files when communicating with the SAP system.

The installation and configuration procedures required on the SAP system must be performed by a BASIS expert who is familiar with the Change and Transport system and who has administrative rights to the SAP system. The exact procedure for importing transport files varies, depending upon the version of BASIS that you are running. For specific procedural details, refer to your SAP documentation.

When you first deploy the Data Access component, all users can access all of your SAP tables by default. To secure the SAP data that users can access, use the Security Definition Editor.

After you have imported transports, you must configure the appropriate levels of user access. Create the required authorizations and apply them through profiles or roles to SAP users who will be designing, running, or scheduling Crystal reports.

Related Information

Creating and applying authorizations [page 757]

24.1.1.17.2.1 Types of transports

There are two different sets of the transports: Unicode compatible transports and ANSI transports. If you are running a BASIS system of 6.20 or later, use the Unicode compatible transports. If you are running a BASIS system earlier than 6.20, use the ANSI transports. All the installed transports are located in the following directory on your product distribution: `Collaterals\Add-Ons\SAP\Transports`. The `transports.txt` file lists the Unicode compatible and ANSI transport files.

Transport types are described below:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Open SQL Connectivity transport
  The Open SQL Connectivity transport enables the Open SQL driver to connect to and report off the SAP system.
- Row-level Security Definition transport
  This transport provides the Security Definition Editor, which is a tool that serves as a graphical interface to the /crystal/auth tables in the Open SQL Connectivity transport.
- Cluster Definition transport
  This transport provides the Cluster Definition tool. This tool enables you to build up a metadata repository for ABAP data cluster definitions. These definitions provide the Open SQL driver with the information it requires in order to report off these data clusters.

  > **Note**
  >
  > ABAP data clusters are not the same as cluster tables. Cluster tables are already defined in the DDIC.

- InfoSet Connectivity transport
  The InfoSet Connectivity transport enables the InfoSet driver to access InfoSets and SAP Queries.
- Content Administration Workbench transport
  This transport provides content administration functionality for BW systems. It is available only as a UNICODE compatible transport.
- BW Query parameter personalization transport
  This transport provides support for personalized and default parameter values in reports based on BW queries.
- BW MDX connectivity transport
  This transport enables the MDX Query driver to access BW cubes and queries. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.
- ODS connectivity transport
  This transport enables the ODS Query driver to access ODS data. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.

24.1.1.17.2.2 Checking for conflicts

The contents of the transport files are registered automatically under the SAP BusinessObjects namespace when you import the files. The SAP BusinessObjects namespace is reserved for this purpose within recent versions of R/3 and MYSAP ERP. However, object names for some objects such as authorization objects, authorization classes, and legacy objects may not contain the appropriate prefixes. It is recommended that you check these object types for conflicts prior to importing the transport files.

If the function group, any of the function modules, or any of the other objects already exists on the SAP system, then you must resolve the namespace before importing the SAP BusinessObjects transport files. Refer to your SAP NetWeaver technology platform documentation for the procedures appropriate to your version of SAP.

24.1.1.17.2.3 Importing the transport files

Read the `transports_EN.txt` file located in the following directory on your product distribution media: `\Collaterals\Add-Ons\SAP\Transports\`. This text file lists the exact names of the files that make up each

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

transport. (The `cofiles` and `data` directories below the `transports` directory correspond to the .../`trans`/`cofiles` and .../`trans`/`data` directories on your SAP server.)

You must import the Open SQL Connectivity transport before importing the Row-level Security Definition or the Cluster Definition transports. You may import the other transports in any order.

> **Note**
>
> After copying files from CD to server, ensure that all files are writable before you import the transports. Imports fail if the import files are read-only.

> **Note**
>
> Because the transports are binary files, on UNIX installations you must add the files by FTP in Binary mode (to avoid file corruption). In addition, you must have write permissions for the UNIX server.

24.1.1.17.2.4 Transports

24.1.1.17.2.4.1 Open SQL Connectivity transport

The Open SQL Connectivity transport enables the drivers to connect to and report off the SAP system.

Table 97:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/OPENSQL	Function group	Open SQL functions
/CRYSTAL/OSQL_AUTH_FORMS	Program	Helper program
/CRYSTAL/OSQL_EXECUTE	Program	Helper program
/CRYSTAL/OSQL_TYPEPOOLPROG	Program	Helper program
/CRYSTAL/OSQL_TYPEPOOLS	Program	Helper program
/CRYSTAL/OSQL_UTILS	Program	Helper program
ZSSI	Authorization object class	Reporting authorization objects
ZSEGREPORT	Authorization object	Reporting authorization object
/CRYSTAL/OSQL_CLU_ACTKEY_ENTRY	Table	Cluster metadata
/CRYSTAL/OSQL_FCN_PARAM	Table	Function metadata

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object	Type	Description
/CRYSTAL/OSQL_FCN_PARAM_FIELD	Table	Function metadata
/CRYSTAL/OSQL_FIELD_ENTRY	Table	Table metadata
/CRYSTAL/OSQL_OBJECT_ENTRY	Table	Table metadata
/CRYSTAL/OSQL_RLS_CHK_ENTRY	Table	RLS metadata
/CRYSTAL/OSQL_RLS_FCN_ENTRY	Table	RLS metadata
/CRYSTAL/OSQL_RLS_VAL_ENTRY	Table	RLS metadata
ZCLUSTDATA	Table	Cluster metadata
ZCLUSTID	Table	Cluster metadata
ZCLUSTKEY	Table	Cluster metadata
ZCLUSTKEY2	Table	Cluster metadata
/CRYSTAL/AUTHCHK	Table	RLS metadata
/CRYSTAL/AUTHFCN	Table	RLS metadata
/CRYSTAL/AUTHKEY	Table	RLS metadata
/CRYSTAL/AUTHOBJ	Table	RLS metadata
/CRYSTAL/AUTHREF	Table	RLS metadata
ZSSAUTHCHK	Table	Old RLS metadata
ZSSAUTHOBJ	Table	Old RLS metadata
ZSSAUTHKEY	Table	Old RLS metadata
ZSSAUTHREF	Table	Old RLS metadata
ZSSAUTH FCN	Table	Old RLS metadata

24.1.1.17.2.4.2 InfoSet Connectivity transport

The InfoSet Connectivity transport enables the InfoSet driver to access InfoSets. This transport is compatible with R/3 4.6c and later. Do not import this transport if you are running SAP R/3 4.6a or earlier.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 98:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/FLAT	Function group	InfoSet wrapper functions
/CRYSTAL/QUERY_BATCH	Program	Batch mode execution
/CRYSTAL/QUERY_BATCH_STREAM	Program	Streaming batch mode execution.

24.1.1.17.2.4.3 Row-level Security Definition transport

This transport provides the Security Definition Editor, which is a tool that serves as a graphical interface to the /CRYSTAL/AUTH tables in the Open SQL Connectivity transport.

Table 99:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/TABMNT	Function group	Function group for table maintenance view for function restrictions
/CRYSTAL/RLSDEF	Program	Main program
/CRYSTAL/RLS_INCLUDE1	Program	Include program containing the module definitions
/CRYSTAL/RLS_INCLUDE2	Program	Include program containing the subroutine definitions
TDDAT [/CRYSTAL/AUTHFCN]	Table contents	Table maintenance definition
TVDIR [/CRYSTAL/AUTHFCN]	Table contents	Table maintenance definition
/CRYSTAL/AUTHFCNS	Definition of transport and maintenance object	Table maintenance definition
/CRYSTAL/RLS	Transaction	Main program transaction
/CRYSTAL/RLSFCN	Transaction	Helper transaction called internally by main program.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.17.2.4.4 Cluster Definition transport

This transport provides the Cluster Definition tool. This tool enables you to build up a metadata repository for ABAP data cluster definitions. These definitions provide the Open SQL driver with the information it requires in order to report off these data clusters.

> **Note**
>
> ABAP data clusters are not the same as cluster tables. Cluster tables are already defined in the DDIC.

Table 100:

Object	Type	Description
ZCIMPRBG	Program	Main program
ZCRBGTOP	Program	Include program
ZCDD	Transaction	Main program transaction

24.1.1.17.2.4.5 Content Administration Workbench transport

This transport provides content administration functionality for BW systems. It is available only as a Unicode compatible transport.

Table 101:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/CL_BW_HTTP_HANDLER	Class	Multi CE-aware HTTP request handler
/CRYSTAL/OBJECT_STATUS_DOM	Domain	Report activity
/CRYSTAL/OBJ_POLICY_DOM	Domain	CE object security
/CRYSTAL/OBJECT_STATUS	Data element	Report activity
/CRYSTAL/OBJ_POLICY	Data element	CE object security
/CRYSTAL/CE_SYNCH	Function group	Publisher stubs
/CRYSTAL/CA_MSG	Message class	Status messages
/CRYSTAL/CE_SYNCH_FORMS	Program	Program component
/CRYSTAL/CONTENT_ADMIN	Program	Program component

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object	Type	Description
/CRYSTAL/ CONTENT_ADMIN_CLASS_D	Program	Program component
/CRYSTAL/CONTENT_ADMIN_CLASS_I	Program	Program component
/CRYSTAL/CONTENT_ADMIN_CTREE	Program	Program component
/CRYSTAL/CONTENT_ADMIN_FORMS	Program	Program component
/CRYSTAL/ CONTENT_ADMIN_MODULES	Program	Program component
/CRYSTAL/CONTENT_ADMIN_PAIS	Program	Program component
/CRYSTAL/CONTENT_ADMIN_PBOS	Program	Program component
/CRYSTAL/ CONTENT_ADMIN_TAB_FRM	Program	Program component
/CRYSTAL/CONTENT_ADMIN_TOP	Program	Program component
/CRYSTAL/PUBLISH_WORKER	Program	Program component
/CRYSTAL/PUBLISH_WORKER_DISP	Program	Program component
/CRYSTAL/PUBLISH_WORKER_DISP_I	Program	Program component
/CRYSTAL/PUBLISH_WORKER_FORMS	Program	Program component
/CRYSTAL/PUBLISH_WORKER_PROC	Program	Program component
/CRYSTAL/ PUBLISH_WORKER_PROC_I	Program	Program component
/CRYSTAL/ PUBLISH_WORKER_SCREEN	Program	Program component
/CRYSTAL/CA_DEST	Table	Application state
/CRYSTAL/CA_JOB	Table	Application state
/CRYSTAL/CA_JOB2	Table	Application state
/CRYSTAL/CA_LANG	Table	Application state
/CRYSTAL/CA_PARM	Table	Application state
/CRYSTAL/CA_ROLE	Table	Application state
/CRYSTAL/CA_SYST	Table	Application state

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object	Type	Description
/CRYSTAL/MENU_TREE_ITEMS	Structure	Application state
/CRYSTAL/REPORT_ID	Table	Application state
/CRYSTAL/RPTADMIN	Transaction	Main program transaction
/CRYSTAL/EDIT_REPORT	Program	Wrapper for report edit
/CRYSTAL/EDIT_REPORT	Function Group	Functions for report edit
ZSSI	Authorization object class	Crystal Authorizations
ZCNTADMCES	Authorization object	CE operations
ZCNTADMRPT	Authorization object	Report operations
ZCNTADMJOB	Authorization object	Background job operations

24.1.1.17.2.4.6 ODS connectivity transport

This transport enables the ODS Query driver to access ODS data. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.

Table 102:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/ODS_REPORT	Function group	ODS functions

24.1.1.17.2.4.7 BW Query parameter personalization transport

This transport provides support for personalized and default parameter values in reports based on BW queries.

Table 103:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/PERS_VAR	Structure	Variable definition
/CRYSTAL/PERS_VALUE	Structure	Value definition

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object	Type	Description
/CRYSTAL/PERS	Function Group	Personalization functions

24.1.1.17.2.4.8 BW MDX connectivity transport

This transport enables the MDX Query driver to access BW cubes and queries. This transport is compatible with BW 3.0B patch 27 or higher and BW 3.1C patch 21 or higher.

Table 104:

Object	Type	Description
/CRYSTAL/BC	Package	Development class
/CRYSTAL/MDX	Function group	MDX functions
/CRYSTAL/MDX_STREAM_LAYOUT	Table definition	Dataset structure
/CRYSTAL/CX_BAPI_ERROR	Class	Exception
/CRYSTAL/CX_METADATA_ERROR	Class	Exception
/CRYSTAL/CX_MISSING_STREAMINFO	Class	Exception
/CRYSTAL/CX_NO_MORE_CELLS	Class	Exception
/CRYSTAL/CX_NO_MORE_MEMBERS	Class	Exception
/CRYSTAL/CX_NO_MORE_PROPER-TIES	Class	Exception
/CRYSTAL/CX_SAVE_SESSION_STATE	Class	Exception
/CRYSTAL/MDX_APPEND_DATA	Class	Dataset processor
/CRYSTAL/MDX_READER_BASE	Class	Dataset processor
/CRYSTAL/MDX_READ_DIMENSIONS	Class	Dataset processor
/CRYSTAL/MDX_READ_MEASURES	Class	Dataset processor
/CRYSTAL/MDX_READ_PROPERTIES	Class	Dataset processor
/CRYSTAL/MDX_AXIS_LEVELS	Table type	Metadata structure
/CRYSTAL/MDX_PROPERTY_KEYS	Table type	Metadata structure
/CRYSTAL/MDX_PROPERTY_VALUES	Table type	Metadata structure

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Object	Type	Description
/CRYSTAL/ MDX_STREAM_LAYOUT_TAB	Table type	Metadata structure

24.1.1.18 Authorizations overview

This section provides a list of SAP authorizations that, in our experience and in our test environment, are required when carrying out common BI platform tasks in an integrated SAP environment. Additional authorization objects or fields may be required, depending upon your individual implementation.

From each authorization object, you must create an authorization and define the appropriate field values. You then apply the appropriate authorizations to the profiles (or roles) of your SAP users. The following sections describe the required authorizations and provide you with the necessary field values. For procedural details that are specific to your version of SAP, refer to your SAP documentation.

> **Note**
>
> The information in this section is provided as a guideline only.

> **Note**
>
> The ZSEGREPORT authorization object belongs to the ZSSI object class, which is installed when you import the SAP Integration transport files needed to support Open SQL queries.

24.1.1.18.1 Creating and applying authorizations

You must create and apply the authorizations needed by each user to access information using the Desktop Intelligence Integration for SAP. The exact procedures for creating, configuring, and applying authorizations depend upon the version of SAP that you have installed. This section provides a list of SAP authorizations that, in our experience and in our test environments, are required when carrying out common tasks when using the BI platform integrated within an SAP NetWeaver ABAP environment. Additional authorization objects or fields may be required, depending upon your individual implementation.

Related Information

Configuring publishing in the Content Administration Workbench [page 737]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19 Actions in BW

This section guides you through a list of various actions in BW.

24.1.1.19.1 Actions within Crystal Reports

24.1.1.19.1.1 Creating a new report from a query in a BW role

Table 105:

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

* **<QUERY_OWNER >** denotes the name of the owner of the query. If you specify a name, you can report off only those queries with that owner. Enter * to report off of queries with any owner.

For **<INFO_AREA>, **<INFO_CUBE>**, or **<COMP_ID >**enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.1.2 Opening an existing report from a BW role

Table 106:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI. RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/ PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.1.3 Previewing or refreshing a report

Table 107:

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Values
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **< INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.1.4 Verifying the database (refreshing table definitions in a report)

Table 108:

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.1.5 Setting the location of the data source

Table 109:

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.1.6 Saving a report to a BW role

Table 110:

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.1.7 Preparing a report for translation while saving to BW

Table 111:

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

24.1.1.19.1.8 Saving a report and simultaneously publishing it to the BI platform

Table 112:

Authorization object	Field	Values
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** ***
	RSINFOCUBE	**<INFO_CUBE>** ***
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** ***
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** ***
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** **
	ACTVT	16

* **<USER_ROLE>** denotes the name of any role that the user belongs to. You can enter multiple values in this field.

** **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

*** For **<INFO_AREA>**, **<INFO_CUBE>**, or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.1.9 Starting the BEx Query Designer™

Table 113:

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERY_OWNER>** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>**, **<INFO_CUBE>**, or **<COMP_ID>**, enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.2 Actions within BI launch pad

24.1.1.19.2.1 Logging on to the BI platform with SAP credentials

Table 114:

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.2.2 Viewing an SAP BW report on demand

Table 115:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>** **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.2.3 Refreshing a report from the viewer

Table 116:

Authorization object	Field	Values
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Values
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>** **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>**, **<INFO_CUBE>**, or **<COMP_ID>**, enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.2.4 Scheduling a report

Table 117:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Values
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>** **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER >** denotes the name of the owner of the query from which you are creating the report. If you enter the name of the query owner, you can only report off of queries with this owner. Enter * to denote any query owner.

** For **<INFO_AREA>** , **<INFO_CUBE>** , or **<COMP_ID>** enter * to denote any value. If you specify a specific value, you can only report off of queries that contain these info areas, cubes, and component IDs.

24.1.1.19.2.5 Reading dynamic picklists in report parameters

Table 118:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

24.1.1.19.3 Actions within SAP NetWeaver (ABAP)

24.1.1.19.3.1 From within Crystal Reports using the Open SQL driver

This section guides you through a list of various actions in SAP NetWeaver (ABAP) from within Crystal Reports using the Open SQL driver.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.3.2 Logging onto an SAP server

Table 119:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

24.1.1.19.3.3 Creating a new report

Table 120:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

24.1.1.19.3.4 Opening or previewing an existing report

Table 121:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.3.5 Verifying the database (refreshing table definitions in a report)

Table 122:

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

24.1.1.19.3.6 Setting the location of the data source

Table 123:

Authorization object	Field	Values
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

24.1.1.19.4 Actions within Crystal Reports using InfoSet driver and reporting off InfoSet

24.1.1.19.4.1 Logging onto an SAP server

Table 124:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.4.2 Creating a new report from an InfoSet on SAP NetWeaver (ABAP)

Table 125:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

> **Note**
>
> Also add enough authorizations to view data rows. For example, P_ORIG or P_APAP.

Related Information

Setting the location of the data source [page 769]

24.1.1.19.4.3 Verifying the database (refreshing table definitions in a report)

Table 126:

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

24.1.1.19.4.4 Setting the location of the data source

Table 127:

Authorization object	Field	Values
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Values	
		COARS	2

24.1.1.19.5 Actions within Crystal Reports using InfoSet driver and reporting off an ABAP query

24.1.1.19.5.1 Logging onto an SAP server

Table 128:

Authorization object	Field	Values
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

24.1.1.19.5.2 Creating a new report from an ABAP query on SAP NetWeaver

Table 129:

Authorization object	Field	Values
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_TABU_DIS	ACTVT	03
	GROUP	Name of table group

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.5.3 Verifying the database

Table 130:

Authorization object	Field	Values
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

24.1.1.19.5.4 Setting the location of the data source

Table 131:

Authorization object	Field	Values
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Name of table group

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.1.1.19.6 Actions within the BI platform

24.1.1.19.6.1 Scheduling a report in dialog mode (with an Open SQL query)

Table 132:

Authorization object	Field	Values
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

> **Note**
>
> The value for CLASS is BLANK.

24.1.1.19.6.2 Scheduling a report in batch mode using an Open SQL query

Table 133:

Authorization object	Field	Values
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Authorization object	Field	Values
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

> **Note**
>
> The value for CLASS is BLANK.

24.1.1.19.6.3 Crystal entitlement system

Table 134:

Authorization object	Field	Value
Authorization for file access (S_DATA-SET)	Activity (ACTVT)	Read, Write (33, 34)
	Physical file name (FILENAME)	* (denotes All)
	ABAP program name (PROGRAM)	*
Authorization Check for RFC Access (S_RFC)	Activity (ACTVT)	16
	Name of RFC to be protected (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY
	Type of RFC object to be protected (RFC_TYPE)	Function group (FUGR)
User Master Maintenance: User Groups (S_USER_GRP)	Activity (ACTVT)	Create or Generate, and Display (03)
	User group in user master maintenance (CLASS)	* **Note** For greater security, you may prefer to explicitly list the user groups whose members require access to the BI platform.

24.1.1.19.6.4 Running and designing BW BEx queries

When creating a report from a universe based on a BW BEx query, if a date dimension is included, the system administrator needs to grant `S_RS_IOBJ` authorization to both the user designing the Universe and the user running the report.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 135:

Authorization object	Field	Values
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

24.2 Configuring for JD Edwards integration

24.2.1 Configuring Single Sign-on (SSO) for SAP Crystal Reports

By default, the BI platform will be configured to allow SAP Crystal Reports users to access JD Edwards EnterpriseOne data using Single Sign-on (SSO).

24.2.1.1 To deactivate SSO for JD Edwards and SAP Crystal Reports

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select *crdb_pseone*.
5. Click *Remove*.
6. Click *Save & Close*.
7. On the *Servers* page in the CMC, select *Crystal Reports Services* and click *Restart server*.

24.2.1.2 To activate SSO for JD Edwards and SAP Crystal Reports

If you have deactivated SSO for JD Edwards and SAP Crystal Reports and wish to reactivate it.

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Under *Use SSO context for database logon with the following drivers*, type *crdb_pseone*.
5. Click *Add*.
6. Click *Save & Close*.
7. On the *Servers* page in the CMC, select *Crystal Reports Services* and click *Restart server*.

24.2.2 Configuring Secure Sockets Layer for JD Edwards Integrations

You can use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your BI platform and JD Edwards EnterpriseOne deployment.

Using JD Edwards EnterpriseOne data with the BI platform requires some changes to your SSL configuration. Similar to the SSL configuration for other BI platform servers and clients, store the following key and certificate files in a secure location (under the same directory) that can be accessed by the computers in your BI platform deployment.

- The trusted certificate file (cacert.der).
- The generated server certificate file (servercert.der).
- The server key file (server.key).
- The passphrase file (passphrase.txt).

24.2.2.1 To enable JD Edwards EnterpriseOne data connectivity with SSL

> **Note**
>
> All values described in the following procedure are case-sensitive.

1. Copy your SSL certificates to `C:\SSLCert`.
2. Start the Central Configuration Manager (CCM).
3. Stop the Server Intelligence Agent (SIA).
4. Double-click the SIA to open the *Properties* dialog box.
5. Click the *Protocol* tab.
6. Select *Enable SSL*.
7. For the *SSL Certificates Folder*, choose the directory containing the SSL certificates: `C:\SSLCert`.
8. For the *Server SSL Certificate File*, choose `servercert.der`.
9. For the *SSL Trusted Certificates Files*, choose `cacert.der`.
10. For the *SSL Private Key File*, choose `server.key`.
11. For the *SSL Private Key Passphrase File*, choose `passphrase.txt`.
12. Click *Apply*.
13. Start the Server Intelligence Agent.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

You must restart your BI platform reporting servers (such as the Adaptive Job Server) before these changes will take effect.

24.2.2.2 SSL configuration property file

The property file `sslconf.properties` contains all the information for required certificates and keys used by the BI platform. For example:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

The `sslconf.properties` file should be put in the folder where the BI platform is installed, `C:\Program Files\Business Objects\BusinessObjects 13.0` by default.

24.3 Configuring for PeopleSoft Enterprise integration

24.3.1 Configuring Single Sign-on (SSO) for SAP Crystal Reports and PeopleSoft Enterprise

By default, the BI platform will be configured to allow SAP Crystal Reports users to access PeopleSoft Enterprise data using Single Sign-on (SSO).

24.3.1.1 To deactivate SSO for PeopleSoft Enterprise and SAP Crystal Reports

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select *crdb_psenterprise*.
5. Click *Remove*.
6. Click *Save & Close*.
7. On the *Servers* page in the CMC, select *Crystal Reports Services* and click *Restart server*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.3.1.2 To activate SSO for PeopleSoft Enterprise and SAP Crystal Reports

If you have deactivated SSO for PeopleSoft Enterprise and SAP Crystal Reports and wish to reactivate it.

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Under *Use SSO context for database logon with the following drivers*, type *crdb_psenterprise*.
5. Click *Add*.
6. Click *Save & Close*.
7. On the *Servers* page in the CMC, select *Crystal Reports Services* and click *Restart server*.

24.3.2 Configuring Secure Sockets Layer communication

You can use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your BI platform deployment.

Similar to the SSL configuration for other BI platform servers and clients, store the following key and certificate files in a secure location (under the same directory) that can be accessed by the machines in your BI platform deployment.

- The trusted certificate file (cacert.der).
- The generated server certificate file (servercert.der).
- The server key file (server.key).
- The passphrase file (passphrase.txt).

24.3.2.1 SSL configuration property file

The property file `sslconf.properties` contains all the information for required certificates and keys used by BI platform components. For example:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

The `sslconf.properties` file should be put in the folder where the BI platform is installed: `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\` by default.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.3.2.2 To enable PeopleSoft Query Server with SSL

> **Note**
>
> All values described in the following procedure are case-sensitive.

1. Copy your SSL certificates to `C:\SSLCert`.
2. Start the Central Configuration Manager (CCM).
3. Stop the Server Intelligence Agent (SIA).
4. Double-click the SIA to open the *Properties* dialog box.
5. Click the *Protocol* tab.
6. Select *Enable SSL*.
7. For the *SSL Certificates Folder*, choose the directory containing the SSL certificates: `C:\SSLCert`.
8. For the *Server SSL Certificate File*, choose `servercert.der`.
9. For the *SSL Trusted Certificates Files*, choose `cacert.der`.
10. For the *SSL Private Key File*, choose `server.key`.
11. For the *SSL Private Key Passphrase File*, choose `passphrase.txt`.
12. Click *Apply*.
13. Start the Server Intelligence Agent.

You must restart your BI platform reporting servers (such as the Adaptive Job Server) before these changes will take effect.

24.3.2.3 To enable Security Bridge with SSL

> **Note**
>
> All values described in the following procedure are case-sensitive.

1. Copy your SSL certificates to `C:\SSLCert`.
2. Start the Central Configuration Manager (CCM).
3. Stop the Server Intelligence Agent (SIA).
4. Double-click the SIA to open the *Properties* dialog box.
5. Click the *Protocol* tab.
6. Select *Enable SSL*.
7. For the *SSL Certificates Folder*, choose the directory containing the SSL certificates: `C:\SSLCert`.
8. For the *Server SSL Certificate File*, choose `servercert.der`.
9. For the *SSL Trusted Certificates Files*, choose `cacert.der`.
10. For the *SSL Private Key File*, choose `server.key`.
11. For the *SSL Private Key Passphrase File*, choose `passphrase.txt`.
12. Click *Apply*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

13. Start the Server Intelligence Agent.

24.3.3 Performance Tuning for PeopleSoft systems

To ensure optimal performance when you report off PeopleSoft queries, it is important to understand how queries are executed by Crystal Reports and the BI platform.

Whenever you refresh or run a report that is based on a PeopleSoft query, a connection is made to a PeopleSoft server:

- In PeopleSoft Enterprise (PeopleTools 8.46 or newer) environments, a connection is made to the *PeopleSoft Analytic Server*.
- In PeopleSoft Enterprise (PeopleTools 8.21-8.45) environments, a connection is made to the *PeopleSoft Application Server*.

24.3.3.1 Recommendations

In an optimal deployment, one or more PeopleSoft Analytic or Application Servers are set up to handle only report requests. In each of these servers, the settings for Min and Max Instances control the number of report requests that can be processed at any one time. This setup provides the following advantages:

- There is no contention between report requests and other transactional requests in the PeopleSoft server.
- It is possible to perform maintenance on the server that handles report requests without disabling the server that handles transactional requests.

In an environment where both report and transactional requests are handled by the same PeopleSoft Analytic or Application Server, you must configure the BI platform not to run more than one report at the same time. Otherwise, users will not be able to make any transactional requests if all of the PSANALYTICSRV or PSAPPSRV processes are used to run reports.

> **Note**
>
> For information on how to limit the number of scheduled report jobs and view-report-on-demand jobs, see "Managing and Configuring Servers" in the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

> **Note**
>
> It is not possible to configure the system to limit the number of Crystal Reports users who may try to access the server at the same time.

If performance issues arise, use the Psadmin configuration tool to determine if requests are being queued. As well, monitor the system resources on the PeopleSoft Analytic or Application Server machine. If virtual memory is being used because of a lack of physical memory, then processing may also slow down.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.3.3.2 PeopleSoft servers

In a PeopleSoft Analytic Server, the process that refreshes or runs the reports is the PSANALYTICSRV process. In a PeopleSoft Application Server, the process that refreshes or runs the reports is the PSAPPSRV process. The number of available PSANALYTICSRV or PSAPPSRV processes determines the number of reports that you can run simultaneously.

A typical PeopleSoft Analytic or Application Server configuration file contains the following information:

```
Min Instances=3
Max Instances=5
```

In this example, a minimum of three PSANALYTICSRV or PSAPPSRV processes are available at any time with the ability to increase to up to five processes. The settings do not necessarily mean that five reports can always be run at the same time; the processes may also be used to handle other tasks in the system. If no PSANALYTICSRV or PSAPPSRV processes are available to handle a request, then the request is queued until a process becomes available.

> **Note**
>
> The configuration file for PeopleSoft *Application* Servers also typically includes the `Service Timeout` parameter, which specifies how long queued requests wait for an available process. If no process becomes available within the time that is specified for the parameter, then the request times out.

24.4 Configuring for Siebel integration

24.4.1 Configuring Siebel to integrate with SAP BI platform

The BI platform integration provides a link to Crystal Reports that allows you to embed SAP BusinessObjects Business Intelligence suite content into a Siebel application. Once installed and configured, the new menu item allows users to launch BI launch pad from within the Siebel application.

By default, the files required are installed in the following folder: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

24.4.1.1 To import the BI platform Siebel integration project

1. Start Siebel Tools.
2. Click *Tools* > *Import from Archive*.
3. When prompted for an archive file, browse to the Siebel Files folder of your Integration product installation.
   By default this is: **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Go to the appropriate subfolder (either Siebel 7.7 or Siebel 8.0) and select the `BusinessObjectsEnterprise.sif` file.
   The Import Wizard appears.
5. Click *Merge the object definition from the archive file with the definition in the repository*.
6. Proceed through the wizard's screens to finish importing the integration project.
   The integration project is added to your repository.
7. Lock the *BusinessObjects Integration* project.

24.4.2 Creating the Crystal Reports menu item

1. In Siebel Tools, lock the *Menu* project.
2. In the Object Explorer, select the *Menu Item* object.

   > **Note**
   >
   > If the Menu object does not appear in the Object Explorer, click *View* > *Options* in Siebel Tools, click the *Object Explorer* tab, and select the *Menu* object.

3. In the *Menus* list, select the *Generic Web* menu.
4. Click the *Menu Items* list heading.
5. Click *Edit* > *New Record*.
6. Define the new menu item appropriately. These are the recommended values:
   - Name: View - Crystal Reports
   - Command: Crystal Reports
   - Comments: SAP BusinessObjects Integrated Report Menu
   - Inactive: False
7. Use a position number to select a location for the menu item in your View menu.

   To help you choose a position number, sort the menu items by Position.
8. You can now add Locale records to localize the caption as appropriate.

Now recompile your Siebel application. See Recompiling the Siebel application [page 781].

24.4.2.1 Recompiling the Siebel application

When you have installed the BI platform and made its command available to users through a Siebel menu item, you must recompile your Siebel application following your usual procedures. For details, see the Siebel Bookshelf.

When you have recompiled your Siebel application, regenerate its JavaScript files. In Siebel 7.7 and later it is possible to automatically regenerate the JavaScript files as part of the recompile process.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Because the steps required to compile the Siebel repository are performed on your Siebel Tools workstation, you need to deploy the resulting JavaScripts from the Siebel Tools workstation to your Siebel Server. Typically, and depending on where Siebel is installed, you can find the generated JavaScript files in the following location:

```
C:\sea77\tools\PUBLIC\ENU\<srf1096416329_444>
```

The example folder name **<srf1096416329_444>** is generated by Siebel Tools, and uniquely corresponds to the resulting repository file.

The JavaScript files should be deployed on the Siebel Server, typically in the following location, depending on where Siebel is installed:

```
C:\sea77\SWEApp\PUBLIC\ENU\<srf1096416329_444>
```

Be sure to maintain the folder name as generated by Siebel Tools.

In addition, you must update your Siebel configuration file on the Siebel Server machine to permit the service. Find the appropriate configuration file on your Siebel Server machine. For example, if you are running an English version of the Siebel Call Center, use `uagent.cfg`. By default, this file is found at `C:\sea77\siebsrvr\bin\ENU\uagent.cfg` for Siebel 7.7.

Then add the following line to the end of the SWE section of the configuration file:

```
ClientBusinessService<NUMBER> = BusinessObjects Integration Service
```

The `ClientBusinessService` numbers are sequential. If there are no other ClientBusinessServices in the SWE section, set **<NUMBER>** to 0. Otherwise, set **<NUMBER>** to be the next highest value.

For Siebel 8.x or higher:

1. Log into Siebel Tools and locate the *Siebel Universal Agent* application object in the Object Explorer.
2. Expand the Application objects to reveal the *Application User Prop* object.
3. Create a new record for each business service to be declared, setting the Name and Value properties for each as shown:
   - Name = ClientBusinessServiceX
   - Value = BusinessObjects Integration

You will now create the Crystal Reports menu item that invokes the imported Siebel command.

24.4.3 Contextual awareness

Contextual awareness is a feature that presents the user with reports that are likely to be relevant to their current task. In this case, users accessing Crystal Reports directly from a Siebel Client application would automatically be show reports that have been designed to incorporate Siebel data.

24.4.3.1 To configure contextual awareness

Before configuring for context sensitivity, make sure you have completed the following.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- installed the Siebel Integration product
- Configured Siebel to integrate with the BI platform

1. Open the Central Management Console (CMC).
2. Click *Authentication*.
3. Double-click *Siebel*.
   The Siebel mapping interface will appear.
4. Click *Domains*.
   The domain mapping interface appears.
5. Make note of the Domain name that corresponds to the Siebel server you want to use.
6. Close the Siebel mapping interface.
7. Open BI launch pad.
8. Create a new folder under `PublicFolders\Siebel` with the same name as the Siebel domain in the CMC.
9. Place any reports that are designed to incorporate Siebel information in this folder.

24.4.3.2 To specify the URL for contextual awareness

1. Once you have regenerated the application's JavaScript files, go to the Siebel Files folder of your BI platform installation, which is by default `C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\`.
2. Copy the `BusinessObjectsEnterpriseServer.html` file. Then find the public folder where the genbscript program generated the new JavaScript files, and place a copy of `BusinessObjectsEnterpriseServer.html` in the appropriate language subfolder.

   For example, if you generated an application's JavaScript files into the `c:\sea752\SWEApp\PUBLIC\ENU` folder on the Siebel server, copy the `BusinessObjectsEnterpriseServer.html` file to the `c:\sea752\SWEApp\PUBLIC\ENU` folder.
3. Open the `BusinessObjectsEnterpriseServer.html` file from the public folder in a text editor such as Notepad, and locate this line:

   ```
   Var userDomain = "SIEB78"
   ```

   ```
   var destAddr = "http://<SAP BusinessObjects server>:8080/BOE/BI/logon/siebelStart.do"
   ```

> **Note**
>
> If you modify the **<userDomain>** or **<destAddr>** variable, you must clear your browser's cached web pages to ensure that the browser will point to the correct destination address.

> **Note**
>
> The userDomain is case-sensitive.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

24.4.3.3 To verify contextual awareness

1. In Siebel Tools, click *Debug* > *Start*.
2. Navigate to any screen and click the *View* menu.
   Your new Crystal Reports menu item should appear on the menu.
3. Click the *Crystal Reports* menu item.
   The BI platform opens the BI launch pad window that requests the username and password to connect to. This is only needed the first time logging on before a session timeout. The domain name configured in html and the Siebel authentication should already be filled in.

> **Note**
>
> This step is only to verify your installation up until this point. You cannot log on to the BI platform using Siebel Authentication until you have mapped Siebel responsibilities to the BI platform.

24.4.3.4 Adding the folders to the BI platform

The BI platform integration for Siebel requires some folders to be added to BI launch pad to fully enable the contextual awareness feature.

In order to function, the contextual folder should have the following structure: `Public Folders\Siebel \<Domain Name>`. Only reports stored in the **<Domain Name>** subfolder and configured in the Siebel system to associate with the specific SAP BusinessObjects business component will display as part of the contextual awareness feature. The **<Domain Name>** used here must be the same domain name configured for Siebel in the Authentication configuration, and the same as the value configured in the Siebel side `BusinessObjectsEnterpriseServer.html` file.

> **Note**
>
> Siebel Tools is required to complete the steps in this section.

24.4.4 Configuring Single Sign-on (SSO) for SAP Crystal Reports and Siebel

By default, the BI platform will be configured to allow SAP Crystal Reports users to access Siebel data using Single Sign-on (SSO).

24.4.4.1 To deactivate SSO for Siebel and Crystal Reports

1. In the Central Management Console (CMC), click *Applications*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. Select *crdb_siebel*.
5. Click *Remove*.
6. Click *Save & Close*.
7. Restart SAP Crystal Reports.

24.4.4.2 To activate SSO for Siebel and SAP Crystal Reports

If you have deactivated SSO for Siebel and SAP Crystal Reports and wish to reactivate it.

1. In the Central Management Console (CMC), click *Applications*.
2. Double-click *Crystal Reports Configuration*.
3. Click *Single Sign-On Options*.
4. *Under Use SSO context for database logon...* type *crdb_siebel*.
5. Click *Add*.
6. Click *Save & Close*.
7. Restart SAP Crystal Reports servers.

24.4.5 Configuring for Secure Sockets Layer Communication

You can use the Secure Sockets Layer (SSL) protocol for all network communication between clients and servers in your Siebel and BI platform deployments.

Similar to the SSL configuration for other BI platform servers and clients, store the following key and certificate files in a secure directory that can be accessed by the machines in your Siebel deployment.

- The trusted certificate file (cacert.der).
- The generated server certificate file (servercert.der).
- The server key file (server.key).
- The passphrase file (passphrase.txt).

SSL configuration property file

The property file `sslconf.properties` contains all the information for required certificates and keys used by the Integration for Siebel components. For example:

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The `sslconf.properties` file should be put in the folder where the BI platform product is installed, `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0` by default.

24.4.5.1 To enable Siebel data connectivity with SSL

> **Note**
>
> All values described in the following procedure are case-sensitive.

1. Copy your SSL certificates to `C:\SSLCert`.
2. Start the Central Configuration Manager (CCM).
3. Stop the Server Intelligence Agent (SIA).
4. Double-click the SIA to open the *Properties* dialog box.
5. Click the *Protocol* tab.
6. Select *Enable SSL*.
7. For the *SSL Certificates Folder*, choose the directory containing the SSL certificates: `C:\SSLCert`.
8. For the *Server SSL Certificate File*, choose `servercert.der`.
9. For the *SSL Trusted Certificates Files*, choose `cacert.der`.
10. For the *SSL Private Key File*, choose `server.key`.
11. For the *SSL Private Key Passphrase File*, choose `passphrase.txt`.
12. Click *Apply*.
13. Start the Server Intelligence Agent.

You must restart your BI platform reporting servers (such as the Adaptive Job Server) before these changes will take effect.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

25 Managing and Configuring Logs

25.1 Logging traces for components

Logs

The BI platform generates system-level messages and writes them to log files. System administrators can use these log files to monitor performance or to debug errors.

Traces

The BI platform also generates traces (recordings of events that occur during the operation of a monitored component) and collects them in log files with the `.glf` extension. Traced events range from status messages to severe exception errors. SAP support staff and developers can use traces to report on the performance of BI platform components (servers and web applications) and the activity of the monitored components.

When you set the trace log level for a component, you determine the type and verbosity of information sent to the log file. The trace log level is a filter that suppresses traces below a specified threshold. By monitoring a component trace log, you can determine whether the current instance of a component or its configuration must be changed to operate under an increased workload.

> **Note**
>
> You can view BI platform log files using any text editor.

25.2 Trace log levels

The following trace log levels are available for BI platform components:

Level	Description
Unspecified	The trace log level is specified through other means (usually an `.ini` file).
None	No tracing occurs.
Low	The trace log filter allows logging error messages while ignoring warning and status messages. Important status messages are logged for component startup, shutdown, start

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Level	Description
	request, and end request messages. This level is not recommended for debugging purposes.
Medium	The trace log filter is set to include error, warning, and most status messages. Least important or highly verbose status messages are filtered out. This level is not verbose enough for debugging purposes.
High	No messages are filtered. This level is recommended for debugging purposes. **Caution** This trace log level significantly affects system resources, increasing CPU usage and consuming storage space.

25.3 Configuring tracing for servers

A log message is a permanent record of events and status of a software system. Traces for a monitored BI platform deployment are written to a specific `.glf` log file and stored in the logging directory.

- On Windows, the default location is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\logging`
- On Unix, the default location is **<INSTALLDIR>**`/sap_bobj/logging`

The name of the `.glf` log file includes a shorthand identifier, the server name, and a number reference, for example, `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. A new trace log file is created for the monitored server once the log file size approaches the ten-megabyte threshold. In addition, five log files are maintained at a time. As new log files are created, old log files are deleted.

You can calibrate the severity and importance of the traces collected in the log file by setting the trace log level for a specific server or group of servers.

Note

To modify the trace log levels for specific servers or group of servers, use the Trace Log Service in the Central Management Console (CMC). To modify other parameters, manually change the trace log level and other settings in the `BO_trace.ini` file.

25.3.1 To set the log level in the CMC

You can adjust the trace log level for a server without affecting other tracing settings.

1. In the *Servers* area of the CMC, access a server.
   - Select a server from a specific category.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- Click *Server List* in the navigation pane to access the complete list of servers, and select a server.

2. Right-click the selected server and select *Properties*.
   The *Properties* dialog box appears.
3. In the *Trace Log Service* area, select a setting from the *Log Level* list.
4. Click *Save & Close*.

The new trace log level takes effect immediately.

To specify a different output directory for log files, include the `-loggingPath <target_directory>` parameter in the *Command Line Parameters* area. Restart the server for this setting to take effect.

Related Information

Trace log levels [page 542]

25.3.2 To set the log level for multiple servers in the CMC

1. In the *Servers* area of the CMC, access multiple servers.
   - Select servers from a specific category.
   - Click *Server List* in the navigation pane to access the complete list of servers. Hold down `Ctrl` and click multiple servers to select them.
2. Right-click the selected servers and select *Edit Common Services*.
   The *Edit Common Services* dialog box is displayed.
3. In the *Trace Log Service* area, select a setting from the *Log Level* list.
4. Click *OK*.

The new trace log level takes effect immediately.

To specify a different output directory for log files, include the `-loggingPath <target_directory>` parameter in the *Command Line Parameters* area. Restart the server for this setting to take effect.

Related Information

Trace log levels [page 542]

25.3.3 To configure server tracing using the BO_trace.ini file

The `BO_trace.ini` file logs only errors and asserts by default.

1. Open the `BO_trace.ini` file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- On Windows, the default location is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\conf\
- On Unix, the default location is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/conf/

2. Uncomment the lines in the "Trace Syntax and Setting" section.
3. Modify the server tracing parameters. The following parameters are used for configuring server tracing:

Parameter	Possible values	Description
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	Determines the severity of log messages. The default log severity is **log_error**. Log severity follows a hierarchy, with **log_information** at the highest level and **log_none** at the lowest. When you set a log severity level, all messages of that level and lower will be displayed. For example, if you set the log severity to **log_warning**, messages including **log_warning**, **log_error**, and **log_fatal** will be written to the log file. **Note** **log_information** and **log_warning** can be shortened to **log_info** and **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Determines the severity of trace messages. The default trace severity is **trace_error**. Trace severity follows a hierarchy, with **trace_debug** at the highest level and **trace_none** at the lowest. When you set a trace severity level, all messages of that level and lower will be displayed. For example, if you set the trace severity to **trace_path**, messages including **trace_path**, **trace_information**, and **trace_error** will be written to the log file. **Note** **trace_information** can be shortened to **trace_info**.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

4. Save and close the `BO_trace.ini` file.

The `BO_trace.ini` file is read frequently. Changes to the `BO_trace.ini` file take effect within five minutes of being saved. If you restart the CMS, changes to the `BO_trace.ini` file will take effect immediately.

Example

`BO_trace.ini` file

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

25.3.3.1 To configure tracing for a specific server

The `BO_trace.ini` file specifies tracing parameters for BI platform servers. The settings affect all managed servers. Administrators can use the `BO_trace.ini` file to set particular tracing parameters for a specific server.

Caution

New trace log level settings specified in the CMC for a specific server will overwrite any settings in `BO_trace.ini`.

1. Open the `BO_trace.ini` file.
   - On Windows, the default location is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On Unix, the default location is **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/conf/`
2. Use an `if` statement to specify tracing settings for a specific server. For example:

```
if (process == "aps_MySIA.ProcessingServer") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

Tip

The process must be specified for the tracing setting to apply to a specific server.

3. Save and close the `BO_trace.ini` file.

The modified settings will be implemented within five minutes.

25.4 Configuring tracing for web applications

Traces for a monitored BI platform deployment are written to a specific `.glf` log file and stored in a directory on the machine that hosts the web application folder.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- On Windows, the default location is `C:\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\` For example, `C:\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- On Unix, the default location is `$userHome/SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>/` For example, `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

The trace log level for web applications in the CMC is set to *Unspecified* by default. Trace Log settings are available for the following applications in the CMC:

- Central Management Console
- BI launch pad
- Open Document
- Web Service

> **Note**
>
> To modify the trace log levels for specific servers or group of servers, use the Trace Log Service in the Central Management Console (CMC). To modify other parameters, manually change the trace log level and other settings in the `BO_trace.ini` file. This file is deployed together with the `BOE.war` and `dswsbobje.war` files on your web application server.

Before you configure the `BO_trace.ini` file, you must use the WDeploy tool to undeploy the existing web applications from your web application server. After you configure the `BO_trace.ini` file, it must be redeployed together with the web applications on your web application server. For more information on using WDeploy to prepare, deploy, and undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.

25.4.1 To set the web application trace log level in the CMC

To trace other web applications, you must manually configure the corresponding `BO_trace.ini` file.

1. In the *Applications* area of the CMC, right-click an application and select *Trace Log Settings*.

   > **Note**
   >
   > These applications have trace log settings: BI launch pad, CMC, Open Document, Promotion Management, Version Management, Visual Difference, and Web Service.

   The *Trace Log Settings* dialog box appears.
2. Select a setting from the *Log Level* list.
3. Click *Save & Close*.

The new trace log level will take effect after the next web application logon.

Related Information

Trace log levels [page 542]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

25.4.2 To configure tracing settings using the BO_trace.ini file

The BO_trace.ini file is deployed with the BOE and dswsbobje .war files on your web application server. You can use the BO_trace.ini to specify tracing parameters for BI platform web applications. Because this file is not always accessible, you must undeploy the affected web application from the web application server.

1. Use WDeploy to undeploy the web application from your web application server. For more information on using WDeploy to undeploy web applications, see the *SAP BusinessObjects Business Intelligence Platform Web Application Deployment Guide*.
   - If you use the Tomcat web application server provided with the BI platform installation, you do not need to undeploy the web applications. You can modify the files directly.
     - The tracing configuration file for the BOE.war file is available at **<INSTALLDIR>**\Tomcat\webapps\BOE\WEB-INF\TraceLog
     - The tracing configuration file for the dswsbobje.war file is available at **<INSTALLDIR>**\Tomcat\webapps\dswsbobje\WEB-INF\conf

   > **Note**
   >
   > If you use the bundled Tomcat web application server, skip step 2.

2. Access a predeployed version of the BO_trace.ini file:
   - The default location of a predeployed version of the configuration file for the BOE.war file is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
   - The default location of a predeployed version of the configuration file for the dswsbobje.war file is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
3. Open the BO_trace.ini file.
   - On Windows, the default location is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\conf\
   - On Unix, the default location is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/conf/
4. Modify the server tracing parameters. The following parameters are used for configuring server tracing:

Parameter	Possible values	Description
sap_log_level	**log_information log_warning log_error log_fatal log_none**	Determines the severity of log messages. The default log severity is **log_error**. Log severity follows a hierarchy, with **log_information** at the highest level and **log_none** at the lowest. When you set a log severity level, all messages of that level and lower will be displayed. For example, if you set the log severity to **log_warning**, messages including **log_warning**,

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Possible values	Description
		log_error, and **log_fatal** will be written to the log file. **Note** **log_information** and **log_warning** can be shortened to **log_info** and **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Determines the severity of trace messages. The default trace severity is **trace_error**. Trace severity follows a hierarchy, with **trace_debug** at the highest level and **trace_none** at the lowest. When you set a trace severity level, all messages of that level and lower will be displayed. For example, if you set the trace severity to **trace_path**, messages including **trace_path**, **trace_info**, and **trace_error** will be written to the log file. **Note** **trace_information** can be shortened to **trace_info**.

5. Save and close the `BO_trace.ini` file.
6. Use WDeploy to deploy the `.war` file on the machine that hosts the web application server.

The modified tracing settings take effect after the next web application logon.

25.4.2.1 To configure tracing for a specific web application

The `BO_trace.ini` file is deployed together with the `BOE` and `dswsbobje .war` files on your web application server. You can use the `BO_trace.ini` to specify tracing parameters for BI platform web applications. Because this file is not always accessible, you must undeploy the affected web application from the web application server. The following are web applications and the `.war` files associated with them:

Web application	WAR file	Predeployed location
Central Management Console	`BOE.war`	**<INSTALLDIR>**`\SAP BusinessObjects Enterprise`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Web application	WAR file	Predeployed location
		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 Business Intelligence Platform Web Application Deployment Guide*.
   - If you use the Tomcat web application server provided with the BI platform installation, you do not need to undeploy the web applications. You can modify the file directly.
     - The tracing configuration file for the BOE.war file is available at **<INSTALLDIR>**\Tomcat\webapps\BOE\WEB-INF\TraceLog
     - The tracing configuration file for the dswsbobje.war file is available at **<INSTALLDIR>**\Tomcat\webapps\dswsbobje\WEB-INF\conf

   > **Note**
   >
   > If you use the bundled Tomcat web application server, skip step 2.

2. Access a predeployed version of the BO_trace.ini file:
   - The default location of a predeployed version of the configuration file for the BOE.war file is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
   - The default location of a predeployed version of the configuration file for the dswsbobje.war file is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
3. Open the BO_trace.ini file.
   - On Windows, the default location is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\conf\
   - On Unix, the default location is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/conf/
4. Use an if statement to specify tracing settings for a specific web application. For example:

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
  sap_trace_level=trace_path;
}
```

The process must be specified for the tracing setting to apply to a specific web application server. The following web applications are available after initial installation:

Web Application	Device Name
BI Launch Pad	**WebApp_BIlaunchpad**
Central Management Server	**WebApp_CMC**
OpenDocument	**WebApp_OpenDocument**

The following parameters are used for configuring web application server tracing:

Parameter	Possible values	Description
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	Determines the severity of log messages. The default log severity is **log_error**. Log severity follows a hierarchy, with **log_information** at the highest level and **log_none** at the lowest. When you set a log severity level, all messages of that level and lower will be displayed. For example, if you set the log severity to **log_warning**, messages including **log_warning**, **log_error**, and **log_fatal** will be written to the log file. **Note** **log_information** and **log_warning** can be shortened to **log_info** and **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Determines the severity of trace messages. The default trace severity is **trace_error**. Trace severity follows a hierarchy, with **trace_debug** at the highest level and **trace_none** at the lowest. When you set a trace severity level, all messages of that level and lower will be displayed. For example, if you set the trace severity to **trace_path**, messages including **trace_path**, **trace_info**, and **trace_error** will be written to the log file.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Possible values	Description
		Note **trace_information** can be shortened to **trace_info**.

5. Save and close the `BO_trace.ini` file.
6. Use WDeploy to deploy the `.war` file on the machine hosting the web application server.

25.5 Configuring tracing for upgrade management tool

You cannot perform tracing configuration for the upgrade management tool using the CMC. You must perform tracing for the upgrade management tool using the `BO_trace.ini` file.

- On Windows, the default location is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\conf\`
- On Unix, the default location is **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/conf/`

25.5.1 To configure tracing for upgrade management tool

1. Open the `BO_trace.ini` file.
   - On Windows, the default location is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - On Unix, the default location is **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/conf/`
2. Uncomment the required lines under the *Trace Syntax and Setting* section.
3. Use an `if` statement to specify tracing settings. For example:

```
if (process == "upgrademanagementtool") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

> **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 within five minutes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

25.6 Configuring tracing for BI platform client applications

Tracing can be activated on the following clients:

- Universe design tool
- Information design tool
- Web Intelligence Rich Client

You can configure tracing for these components by editing .ini files for each of the client types. These .ini files operate identically to the BO_trace.ini file described elsewhere in this chapter. See To configure server tracing using the BO_trace.ini file [page 789] for details on modifying the .ini file.

The files need to be located in the working directories configured for these applications (`<INSTALLDIR>\SAP BusinessObjects` by default). If they do not already exist, you may need to create them. The files have the following names:

- Universe design tool: `designer_trace.ini`.
- Information design tool: `BO_Trace.ini`
- Web Intelligence Rich Client: `WebIRichClient_trace.ini`

See the documentation for these products for more information.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

26 Integration to SAP Solution Manager

26.1 Integration overview

Supportability features have been added to the BI platform to enable integration into SAP Solution Manager. The following SAP Solution Manager™ components can be used to provide support for your BI platform deployment:

- Solution Landscape Directory
- Solution Manager Diagnostics
- Introscope by CA Wily
- SAP Passport

> **Note**
>
> To access the SAP Support Portal for SAP BusinessObjects go to: https://websmp205.sap-ag.de/bosap-support

26.2 SAP Solution Manager integration checklist

The following table summarizes what components are required to enable SAP Solution Manager to provide support for the BI platform.

Table 136:

SAP Solution Manager Support	Required for the BI platform
SLD registration	• SAPHOSTAGENT must be installed to enable registration of BI platform servers. **Note** The BI platform installer will automatically register servers if SAPHOSTAGENT is already installed. • Must create a connect.key file for the data supplier reporting on the back-end servers. • (Optional) For SLD registration with WebSphere 6.1 or 7, the SLDREG registration tool must be installed on each WebSphere web application server. For more information, refer to SAP Note 1482727. • (Optional) For SLD registration with SAP NetWeaver 7.2, install SLDREG on every NetWeaver host. Refer to SAP Note 1018839 for more information. • (Optional) For SLD registration with Apache Tomcat, SLDREG must be installed on each Tomcat server. For more information, refer to SAP Note 1508421.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Solution Manager Support	Required for the BI platform
SMD integration	• Must download and install SMD Agent (DIAGNOSTICS.AGENT) on all hosts of BI platform servers. • SMAdmin user account must be enabled in the BI platform.
Performance instrumentation	• Introscope Agent must be configured to connect to Enterprise Manager. Use the BI platform installer or CMC node placeholders to configure the connections. • SMD Agent must be installed. • The BI platform must be configured to connect to the SMD Agent. Use the BI platform installer or CMC node placeholders to configure the connections.
SAP Passport	• You need to download and install SAP Passport client tool.

26.3 Managing system landscape directory registration

26.3.1 Registration of the BI platform in the System Landscape

The System Landscape Directory (SLD) is a central repository of system landscape information that is relevant for the management of the software lifecycle. The SLD contain a description of the system landscape - the systems and software components that are currently installed. SLD data suppliers register the systems on the SLD server and keep the information up-to-date. Management and business applications access the information stored in the SLD to perform tasks in a collaborative computing environment.

The System Landscape Directory-Data Supplier (SLD-DS) is the application responsible for registering the BI platform servers into the SLD server. A specific data supplier is provided for every installation of the platform to report on the following components:

- BI platform servers
- Web applications and services hosted on the WebSphere web application server.

> **Note**
>
> SAP NetWeaver has a built-in SLD-DS supplier that registers the NetWeaver application server as well as hosted web applications and services. This SLD-DS is relevant for BI platform deployments that are integrated within an SAP NetWeaver environment.

The SLD-DS that reports on BI platform servers requires that the SLDREG program be installed and configured. The SLDREG program is installed when you install the SAPHOSTAGENT tool. For more information on how to access and install the SAPHOSTAGENT see the Preparation section in the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. Once SLDREG has been installed, you need to create a `connect.key` file to enable it to connect to the SLD server.

For information on how to configure the specific data supplier for WebSphere, see the *Web Application Deployment Guide*.

During the installation of the BI platform, information required for registering the BI platform is stored in a configuration file. This file contains information used by the SLD DS to connect to the BI platform database.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

26.3.1.1 To create a connect.key file for the SLD data supplier

Before creating a `connect.key` file for the SLD data supplier, you need to download and install the SAPHOSTAGENT. See the Preparation section in the *SAP BusinessObjects Business Intelligence Platform Installation Guide* for more details.

> **Note**
>
> The `connect.key` file is required for SLD registration with the data supplier that reports on BI platform servers.

1. Open a command line console.
2. Navigate to the default SAPHOSTAGENT install path.
   - On Windows: `Program Files\SAP\hostctrl\exe`
   - On Unix: `/usr/sap/hostctrl/exe`
3. Run the following command:
   ```
   sldreg -configure connect.key
   ```
4. Enter the following configuration details
   - User name
   - Password
   - Host
   - Port number
   - Specify to use HTTP

The `sldreg` tool will create a connect.key file that will automatically be used by the data supplier to push information to the SLD server.

26.3.2 When is SLD registration triggered?

The SLD registration process is invoked by the data supplier reporting on the BI platform back-end servers in the following scenarios:

- A server node on your BI platform deployment is restarted.
- A new server or a node is added to the deployment.
- A server or a node is deleted

> **Note**
>
> If a server or a node is deleted, the SLD registration process does not modify the contents on the SLD server. To update the SLD server when a server or node is removed, delete the system from the SLD and resend it by restarting the BI platform.

The data supplier for WebSphere SLD registration can be invoked manually or set to run on a specified interval - for example, every 24 hours. For more information on configuring this data supplier refer to SAP Note 482727.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

26.3.3 Logging SLD connectivity

Data supplier configuration file

A configuration file used for SLD registration is created for BI platform deployments. The file, `sldparserconfig.properties`, is located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

Logging SLD connectivity

Connectivity between the SLD server and the data supplier on the BI platform deployment is controlled through the `sldreg` tool and the `connect.key` file.

> **Note**
>
> The log file name is specified as a property in the `sldparserconfig.properties` file.

The log file for the SLD data supplier reporting on the BI platform back-end servers is by default located in the following location: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. The file is overwritten each time the data supplier is executed.

The log files for `sldreg` are by default located in the following location: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. The sldreg log file names cannot be modified, and use the following format: `sldreg_<Timestamp>.log`.

A new log file is created each time the data supplier calls sldreg.

26.4 Managing Solution Management Diagnostics agents

26.4.1 Solution Manager Diagnostics (SMD) overview

The Solution Manager Diagnostics (SMD) component of SAP Solution Manager provides all functionality to centrally analyze and monitor a complete system landscape. The BI platform can be monitored by the SMD server if an SMD Agent is installed. The SMD Agent (`DIAGNOSTICS.AGENT`) gathers information for the SMD which can then be used for root cause analysis. Information collected and sent to the SMD server includes back-end server configurations and the location of server log files.

26.4.2 Working with SMD agents

The BI platform does not install the SMD Agent. The agent, `DIAGNOSTICS.AGENT`, is available to download from the following location: http://service.sap.com/swdc.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Information on installing and configuring the agent is available at: http://service.sap.com/diagnostics

Guidelines for working with the SMD Agent

The following are provided as guidelines for using SMD agents to monitor the BI platform:

- Installation order of monitored system and agent is not important. You can choose to install the SMD Agent before or after installing and deploying the BI platform.
- When installing an SMD Agent, make a note of the host name and listening port. These are critical for configuring the BI platform as a monitored system. If you have installed the agent before the monitored system, you can provide the configuration information during the BI platform installation setup. This information can also be provided later through placeholders for the nodes in the Central Management Console in your deployment.
- If the back-end servers are deployed on a distributed system, you should install an SMD Agent on every machine hosting a back-end server.
- For performance instrumentation of non-java servers, the SMD Agent is required.
- You must activate the SMAdmin user account to enable the SMD Server access the CMS.

26.4.3 SMAdmin user account

Every BI platform deployment has a user account created to facilitate SMD integration. This read-only account is used by the SMD server to log into the CMS and to gather server configuration and other information about the deployment.

The SMAdmin account is deactivated by default.

26.4.3.1 To activate the SMAdmin account

1. In the *Users and Groups* management area of the CMC, select *User List*.
   The list of users is displayed.
2. Locate the *SMAdmin* user account.
3. Click *Manage* > *Properties*.
   The *Properties* dialog box appears.
4. Clear the *Account is disabled* box.
5. Click *Save & Close*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

26.5 Managing performance instrumentation

26.5.1 Performance instrumentation for the BI platform

You can use CA Wily Introscope as part of SAP Solution Manager for measuring BI platform performance instrumentation. When installing the platform, the following resources are provided for your deployment

- Introscope agent: Introscope agents collect performance metrics from BI platform Java back-end severs. Agents also collect information from the surrounding computing environment. The agents then report these metrics to the Enterprise Manager.
- The files provided to facilitate the instrumentation process. One set of files are provided for instrumentation of non-Java servers, and another set of files for instrumentation of Java servers. On the SAP Solution Manager end, the Enterprise Manager (EM) component is required. EM acts as the central repository for all Introscope performance data and metrics collected in an application environment. The EM processes performance data and makes it available to users for production monitoring and diagnosis.

26.5.2 Setting up performance instrumentation for the BI platform

There are two ways to set up performance instrumentation for workflows running on BI platform back-end servers.

1. During the installation setup for the BI platform. You will need to know the hostname and the listening port for the SMD Agent. For more information see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*. If you choose this option, instrumentation will by default run once you have finished deploying the monitored system.
2. After installing the BI platform, you can provide the configuration information for the SMD agent through placeholders in the node properties in the Central Management Console (CMC).

> **Note**
>
> For instrumentation of workflows on non-Java servers, you must have the SMD Agent (`DIAGNOSTICS.AGENT`) installed.

Related Information

Working with SMD agents [page 802]

 © 2015 SAP SE or an SAP affiliate company. All rights reserved.

26.5.2.1 To configure nodes for instrumentation

Use the following instructions if you did not provide configuration information for the SMD Agent and Enterprise Manager during installation setup for the BI platform.

1. Go to the *Servers* area in the CMC.
2. In the navigation pane, click *Nodes*.
   All available nodes are displayed.
3. Right-click the node on which you want to perform instrumentation and select *Placeholders*.
   The Placeholders dialog box appears.
4. Modify the value for the following placeholders.

Placeholder	Description
%IntroscopeAgentEnableInstrumentation%	Enables or disables instrumentation on Java servers. Will be set to enabled if you have provided configuration details for Enterprise Manager during installation setup. Set to `true` to enable instrumentation.
%IntroscopeAgentEnterpriseManagerHost%	Host name for machine on which Enterprise Manager is installed.
%IntroscopeAgentEnterpriseManagerPort%	Listening port used by Enterprise Manager.
%IntroscopeAgentEnterpriseManagerTransport%	Communication protocol used by Enterprise Manager. Supported protocols include TCP, SSL, HTTP Tunnel, and HTTPS.
%NCSInstrumentLevelThreshold%	Used to set the level of instrumentation for non-Java servers. Set to "0" if you want to turn off instrumentation. Set to any value above "0" to activate instrumentation.
%SMDAgentHost%	The hostname of the machine on which the SMD Agent (`DIAGNOSTICS.AGENT`) is installed .
%SMDAgentPort%	The listening port used by the SMD agent.

5. Click *Save&Close*.
6. Restart the node.

After the node is restarted, the new values provided will propagate to all the managed servers.

26.5.3 Performance instrumentation for the web tier

Instrumentation data for web tier components is not included with the BI platform.

26.5.4 Instrumentation log files

Once your BI platform deployment is configured to run instrumentation, messages are logged in specific locations. Checking the log files is a way to verify instrumentation status.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

For instrumentation on Java back-end servers, a log file is located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs`. A separate `.log` file is created for each java process. The folder will also contain `AutoProbe.log` files that specify which methods have been loaded for instrumentation.

For instrumentation on non-Java back-end servers, log files are located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/logging/`. On Unix, the files are located in the `<sap_bobj>\logging\` directory. Instrumentation related log files for non-Java servers are saved as `.trc` files.

For instrumentation on web application servers, a log file is located in the following directory: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. Two types of log files appear in this folder: `Introscope.log` and `Autoprobe.log`.

26.6 Tracing with SAP Passport

In addition to tracing BI platform components such as servers and web applications, the tracing mechanism can support the tracing of a specific action. An end-to-end trace analysis analyzes the performance of a single transaction. The consolidation of all the tracing information for a specific action enables SAP support personnel to see all the tracing data without being distracted by tracing information related to other actions.

SAP Passport

The mechanism supporting the end-to-end tracing for the BI platform is a tool called SAP Passport™. The SAP Passport client tool injects a unique identifier into all HTTP requests for a particular workflow and this identifier is forwarded to all servers used in the workflow. SAP support personnel can put together an end-to-end trace for the workflow by using this unique identifier.

> **Note**
>
> Trace log levels specified in the CMC and the `BO_trace.ini` configuration file are used if they are higher than the levels specified in the SAP Passport client tool - `SAPClientPlugin.exe`.

You can find the Passport in the logs for the back-end servers, web applications, and web services logs.

The SAP Passport client tool is not installed as part of the BI platform. To access and download the tool, go to http://service.sap.com/swdc.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27 Command Line Administration

27.1 Unix scripts

This section details each of the administrative tools and scripts that are included with the Unix distribution of the BI platform. This section is provided primarily for reference purposes. Concepts and configuration procedures are discussed in more detail throughout this guide.

The Unix distribution of the BI platform includes a number of scripts that, together, provide you with all the configuration options that are available in the Windows version of the Central Configuration Manager (CCM). There are a number of other scripts that provide you with Unix-specific options or serve as templates for your own scripts. Also, there are several secondary scripts that are used by the BI platform. Each script is described here and the command-line options are provided where applicable.

> **Note**
>
> When entering Unix command-line parameters, you may need to escape or multiply escape special shell characters. For example, if the exclamation mark "!" is used in a password, you may need to escape the exclamation mark, like this: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

27.1.1 Script utilities

This section describes the administrative scripts that assist you in working with the BI platform on UNIX. The remainder of this section discusses the concepts behind each of the tasks that you can perform with these scripts. This reference section provides you with the main command-line options and their arguments.

27.1.1.1 ccm.sh

The `ccm.sh` script is installed to the **<INSTALLDIR>**`/sap_bobj` directory of your installation. This script provides you with a command-line version of the Central Configuration Manager. This section lists the command-line options and provides some examples.

> **Note**
>
> Arguments in square brackets [ ] are optional.

> **Note**
>
> If you are unsure of a Server Intelligence Agent's name, look at the Command properties in the `ccm.config` file, and use the value that appears after the `-name` option.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The `ccm.sh` script can only be launched by the user that performed the installation of the BI platform.

- Arguments denoted by **<other authentication information>** are provided in the second table.

Table 137:

CCM Option	Valid Arguments	Description
`-help`	n/a	Display command-line help.
`-start`	`all` or **<sianame>**	Start each Server Intelligence Agent as a process. The `all` option starts all of the nodes on the machine, including any nodes belonging to different clusters.
`-stop`	`all` or **<sianame>**	Stop each Server Intelligence Agent by terminating its Process ID. The `all` option starts all of the nodes on the machine, including any nodes belonging to different clusters.
`-restart`	`all` or **<sianame >**	Stop each Server Intelligence Agent by terminating its Process ID; then each SIA is started. The `all` option starts all of the nodes on the machine, including any nodes belonging to different clusters.
`-managedstart`	**<fully qualified server name> <[other authentication information]>**	Start a server.
`-managedstop`	**<fully qualified server name> <[other authentication information]>**	Stop a server.
`-managedrestart`	**<fully qualified server name> <[other authentication information]>**	Stop a server; then start the server.
`-managedforceterminate`	**<fully qualified server name> <[other authentication information]>**	Stops the server immediately without completing current processing requests.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

CCM Option	Valid Arguments	Description
-enable	**<fully qualified server name> <[other authentication information]>**	Enable a started server so that it registers with the system and starts listening on the appropriate port. Use the fully qualified form of the server name.
-disable	**<fully qualified server name> <[other authentication information]>**	Disable a server so that it stops responding to BI platform requests but remains started as a process. Use the fully qualified form of the server name.
-display	**< [other authentication information]>**	Reports the current status of all of the servers in the cluster, including the server names, the host names, Process IDs, descriptions, whether they are running, and whether they are enabled or disabled.

The following table describes the options that make up the argument denoted by **<[other authentication information]>**.

> **Note**
>
> For improved security, you must always provide the credentials of an account with Enterprise authentication. Other types of authentication are not supported.

Table 138:

Authentication Option	Valid arguments	Description
-cms	**<cmsname:port#>**	Specify the CMS that you want to log on to. If not specified, the CCM defaults to the local machine and the default port (6400).
-username	**<username>**	Specify an account that provides administrative rights to BI platform. If not specified, the default Administrator account is attempted.
-password	**<password>**	Specify the corresponding password. If not specified, a blank password is attempted. **Note** To specify the -password argument, you must also specify the -username argument.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The CCM reads the launch strings and other configuration values from the `ccm.config` file.

Related Information

ccm.config [page 810]

27.1.1.1.1 Examples

These two commands start and enable all BI platform servers. The Central Management Server (CMS) is started on the local machine and the default port (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

These two commands start and enable all BI platform servers. The CCM will enable all servers in the cluster, where the CMS runs on machine MACHINE01 and port 6701:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

These two commands start and enable all BI platform servers with a specified administrative account named `SysAdmin` and the provided password:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

This single command logs on with a specified administrative account to disable an Adaptive Job Server that is running on a second machine:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -
password 35%bC5@5
```

27.1.1.1.2 ccm.config

This configuration file defines the launch strings and other values that are used by the CCM when you run its commands. This file is maintained by the CCM itself, and by the other BI platform script utilities. You typically edit this file only when you need to modify a Server Intelligence Agent's command line. It is strongly recommended that you back up this file before editing it manually.

Related Information

Command lines overview [page 817]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27.1.1.2 cmsdbsetup.sh

The `cmsdbsetup.sh` script is installed to the **<sap_bobj>** directory of your installation. The script provides a text-based program that enables you to perform the following tasks.

- Configure a CMS system database
- Reinitialize a CMS system database
- Copy data from another data source
- Change the cluster key
- Change the name of the cluster

> **Note**
>
> Before running this script, back up your current CMS system database and the contents of your Input and Output File Repositories. For more information, see the "Backing up and Restoring Your System". Also be sure to see Clustering Central Management Servers in the "Server Maintenance" chapter of the *SAP BI platform Administrator Guide* for additional information about CMS clusters and configuring the CMS database.

The script will prompt you for the name of your Server Intelligence Agent (SIA). To check the name of your SIA, view the Command properties of the SIA in the `ccm.config` file. The SIA's current name appears after the `-name` option. Or, you can use option 8 with the `serverconfig.sh` file.

Related Information

Clustering Central Management Servers [page 342]
Overview of backup and restore [page 442]

27.1.1.3 serverconfig.sh

The `serverconfig.sh` script is installed to the **<sap_bobj>** directory of your installation. This script provides a text-based program that allows you to perform the following operations.

- Add a node
- Delete a node
- Modify a node
- Move a node
- Back up server configuration
- Restore server configuration
- Modify web tier configuration
- List all nodes

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27.1.1.3.1 To add/delete/modify/list nodes on UNIX

1. Go to the **<INSTALLDIR>**`/sap_bobj` directory of your installation.
2. Issue the following command:

   ```
   ./serverconfig.sh
   ```

   The script prompts you with a list of options:

   1. Add a node
   2. Delete a node
   3. Modify a node
   4. Move a node
   5. Back up server configuration
   6. Restore server configuration
   7. Modify web tier configuration
   8. List all nodes
3. Type the number that corresponds to the action you want to perform.
4. If you are adding, deleting, or modifying a server, provide the script with any additional information that it requests.

27.1.2 Script templates

27.1.2.1 startservers

The `startservers` script is installed to the **<INSTALLDIR>**`/sap_bobj` directory of your installation. This script can be used as a template for your own scripts: it is provided as an example to show how you could set up your own script that starts the BI platform servers by running a series of CCM commands. For details on writing CCM commands for your servers, see ccm.sh [page 807].

27.1.2.2 stopservers

The `stopservers` script is installed to the **<INSTALLDIR>**`/sap_bobj` directory of your installation. This script can be used as a template for your own scripts: it is provided as an example to show how you could set up your own script that stops the BI platform servers by running a series of CCM commands. For details on writing CCM commands for your servers, see ccm.sh [page 807].

27.1.3 Scripts used by the BI platform

These secondary scripts are often run in the background when you run the main BI platform script utilities and you do not need to run them yourself.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

bobjrestart.sh

This script is run internally by the CCM to manage Server Intelligence Agent nodes. Do not run this script yourself.

env.sh

The `env.sh` script is installed to the **<sap_bobj/setup>** directory of your installation. This script sets up the BI platform environment variables that are required by some of the other scripts. BI platform scripts run env.sh as required. See the *SAP BusinessObjects Business Intelligence Platform Installation Guide* for more details.

env-locale.sh

The `env-locale.sh` script is used for converting the script language strings between different types of encoding (for example, UTF8 or EUC or Shift-JIS). This script is run by `env.sh` as needed.

initlaunch.sh

The `initlaunch.sh` script runs `env.sh` to set up the BI platform environment variables, and then runs any command that you have added as a command-line argument for the script. This script is intended primarily for use as a debugging tool by SAP BusinessObjects.

postinstall.sh

The `postinstall.sh` script is installed to the **<SCRIPTDIR>** directory of your installation. You should not run this script yourself.

setup.sh

The `setup.sh` script is installed to the root directory of your installation. This script provides a text-based program that allows you to set up your BI platform installation. This script is run automatically when you install the BI platform. It prompts you for the information that is required in order to set up the BI platform for the first time.

For complete details on responding to the setup script when you install the BI platform, see the *SAP BusinessObjects Business Intelligence Platform Installation Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

setupinit.sh

The `setupinit.sh` script is installed to the **`</sap_bobj/init>`** directory of your installation. This script copies the run control scripts to your `rc#` directories for automated startup. If you want your BI platform servers to start and stop with the machine they are installed on, run this script after the `setup.sh` script completes.

> **Note**
>
> You must have root privileges to run this script.

27.2 Windows scripts

This section details each of the administrative tools and scripts that are included with the Windows distribution of the BI platform. This section is provided primarily for reference purposes. Concepts and configuration procedures are discussed in more detail throughout this guide.

The Windows distribution of the BI platform includes the Windows version of the Central Configuration Manager (CCM). In addition to interacting with the GUI, you can choose to run the CCM executable from the command line with options to manage your servers.

27.2.1 ccm.exe

The `ccm.exe` executable is installed to the **`<INSTALLDIR>`**`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` directory of your installation. You can run the executable directly from the command line to perform certain operations. This section lists the command-line options and provides some examples.

> **Note**
>
> A Server Intelligence Agent (SIA) and Central Management Server (CMS) must be running before using the command-line options of `ccm.exe` to interact with an individual server.

> **Note**
>
> Arguments in square brackets [ ] are optional.

> **Note**
>
> Arguments denoted by **`<other authentication information>`** are provided in the second table.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 139:

CCM Option	Valid Arguments	Description
-help	n/a	Display command-line help.
-managedstart	all or **<fully qualified server name> <[other authentication information]>**	Start a server.
-managedstop	all or **<fully qualified server name> <[other authentication information]>**	Stop a server.
-managedrestart	all or **<fully qualified server name> <[other authentication information]>**	Stop a server; then start the server.
-managedforceterminate	all or **<fully qualified server name> <[other authentication information]>**	Stops the server immediately without completing current processing requests.
-enable	all or **<fully qualified server name> <[other authentication information]>**	Enable a started server so that it registers with the system and starts listening on the appropriate port.
-disable	all or **<fully qualified server name> <[other authentication information]>**	Disable a server so that it stops responding to BI platform requests but remains started as a process.
-display	**< [other authentication information]>**	Reports the current status of all of the servers in the cluster, including the server names, the host names, Process IDs, descriptions, whether they are running, and whether they are enabled or disabled.

The following table describes the options that make up the argument denoted by **<[other authentication information]>**.

> **Note**
>
> You must always provide the credentials of an account with Enterprise authentication.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 140:

Authentication Option	Valid arguments	Description
-cms	**<cmsname:port#>**	Specify the CMS that you want to log on to. If not specified, the CCM defaults to the local machine and the default port (6400).
-username	**<username>**	Specify an account that provides administrative rights to the BI platform. If not specified, the default Administrator account is attempted.
-password	**<password>**	Specify the corresponding password. If not specified, a blank password is attempted. **Note** To specify the -password argument, you must also specify the -username argument.
-authentication	**<authentication type>**	Specify the authentication type. Only **secEnterprise** is supported.

The CCM reads the launch strings and other configuration values from the ccm.config file.

27.2.1.1 Examples

The following examples assume that a Server Intelligence Agent (SIA) and Central Management Server (CMS) are started and running. Before using the command-line options of ccm.exe to interact with an individual server, you can use the following Windows command to start the SIA service:

```
net start "Server Intelligence Agent (NODENAME)"
```

The SIA can also be stopped using net stop "Server Intelligence Agent (NODENAME)".

This command starts all BI platform servers:

```
ccm.exe -managedstart all
```

This command starts an Adaptive Job Server. The CMS was started on port 6701, rather than on the default port:

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

This command enables an Adaptive Job Server with a specified administrative account named SysAdmin:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

This command logs on with a specified administrative account to disable an Adaptive Job Server that is running on a second machine:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin
-password 35%bC5@5
```

27.3 Server Command Lines

27.3.1 Command lines overview

This section lists the command-line options that control the behavior of each BI platform server.

When you start or configure a server through the Central Management Console (CMC) the server is started (or restarted) with a default command line that includes a typical set of options and values. In the majority of cases, you need not modify the default command lines directly. Moreover, you can manipulate the most common settings through the various server configuration screens in the CMC. For reference, this section provides a full listing of the command-line options supported by each server. You can modify each server's command line directly if you need to further customize the behavior of the BI platform.

Throughout this section, values provided in square brackets [ ] are optional.

> **Note**
>
> The following tables list the supported command-line options. BI platform servers use a number of internal options that are not listed in these tables. These internal options must not be modified.

27.3.1.1 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.

27.3.2 Standard options for all servers

These command-line options apply to all of the BI platform servers, unless otherwise indicated. See the remainder of this section for options specific to each type of server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 141:

Option	Valid Arguments	Behavior
`-requestPort`	**`<port>`**	Specify the port that the server listens on. The server registers this port with the CMS. If unspecified, the server chooses any free port greater than 1024. **Note** This port is used for different purposes by different servers. Before changing, see the section on changing the default server port numbers in the *BI platform Administrator Guide*.
`-loggingPath`	**`<absolute path>`**	Specify the path where log files are created.

27.3.2.1 UNIX signal handling

On UNIX, the BI platform daemons handle the following signals:

- `SIGTERM` results in a graceful server shutdown (exit code = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE`, and `SIGILL` result in a rapid shutdown (exit code = 1).

27.3.3 Central Management Server

This section provides the command-line options that are specific to the CMS. The default path to the server on Windows is **`<INSTALLDIR>`**`\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

The default path to the server on UNIX is **`<INSTALLDIR>`**`/sap_bobj/enterprise_xi40/`**`<platform>`**`/boe_cmsd`.

Table 142:

Option	Valid Arguments	Behavior
`-threads`	**`<number>`**	Specifies the number of working threads that the CMS initializes and uses. The value can be between 12 and 150, and is set to 50 by default.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Valid Arguments	Behavior
-reinitializedb		Cause the CMS to delete the system database and recreate it with only the default system objects. All existing data in the database is lost when it is recreated.
-quit		Force the CMS to quit after processing the -reinitializedb option.
-receiverPool	**<number>**	Specify the number of threads the CMS creates to receive client requests. A client may be another SAP BusinessObjects server, the Report Publishing Wizard, Crystal Reports, or a custom client application that you have created. The default value is 5. Normally you will not need to increase this value, unless you create a custom application with many clients.
-maxobjectsincache	**<number>**	Specify the maximum number of objects that the CMS stores in its memory cache. Increasing the number of objects reduces the number of database calls required and greatly improves CMS performance. However, placing too many objects in memory may result in the CMS having too little memory remaining to process queries. The default value is 100000.
-ndbqthreads	**<number>**	Specify the number of CMS worker threads sending requests to the database. Each thread has a connection to the database, so you must be careful not to exceed your database capacity. In most cases, the maximum value you should set is 20.
-oobthreads	**<number>**	If your cluster includes more than eight CMS cluster members, ensure that the command-line for each CMS includes this option. Specify the number of CMS services in your cluster. This option ensures that the cluster can sustain heavy load.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Standard options for all servers [page 817]

27.3.4 Crystal Reports Processing Server and Crystal Reports Cache Server

The Crystal Reports Processing Server and the Crystal Reports Cache Server are controlled in much the same way from the command line. The command-line options determine whether the server starts as a Processing Server, a Cache Server, or both. Options that apply only to one server type are noted below.

The default paths to the servers on Windows are:

- **<INSTALLDIR>**\SAP BusinessObjects Business Intelligence platform 4.0 \win64_x64\cacheserver.exe.
- **<INSTALLDIR>**\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe.

The default paths to the servers on UNIX are:

- **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM>**/boe_cachesd.
- **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM>**/boe_procd.

Table 143:

Option	Valid Arguments	Behavior
-cache		Enable Cache Server functionality.
-deleteCache		Delete the cache directory every time the server starts and stops.
-report_ProcessExtPath	**<absolutepath>**	Specify the default directory for processing extensions.

Related Information

Standard options for all servers [page 817]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27.3.5 Dashboards Processing Server and Dashboards Cache Server

The Dashboards Processing Server and the Dashboards Cache Server are controlled in much the same way from the command line. The command-line options determine whether the server starts as a Processing Server, a Cache Server, or both. Options that apply only to one server type are noted below.

The default paths to the servers on Windows are:

- **<INSTALLDIR>**\SAP BusinessObjects\BI platform 4.0\win64_x64\xccache.exe.
- **<INSTALLDIR>**\SAP BusinessObjects\BI platform 4.0\win64_x64\xcproc.exe.

The default paths to the servers on UNIX are:

- **<INSTALLDIR>**/sap_bobj/enterprise_xi40/<platform>_64/boe_xccached.
- **<INSTALLDIR>**/sap_bobj/enterprise_xi40/<platform>_64/xcprocd.

Table 144:

Option	Valid Arguments	Behavior
-cache		Enable Cache Server functionality.
-dir	**<absolutepath>**	Specify the cache directory for a Cache Server and the temp directory for the Processing Server. The directories created are absolutepath/cache and absolutepath/temp
-deleteCache		Delete the cache directory every time the server starts and stops.
-psdir	**<absolutepath>**	Specify the temp directory for the Processing Server. This option overrides –dir.
-refresh	**<minutes>**	Share cached pages for the specified number of minutes.
-auditMaxEventsPerFile	**<number>**	On the Cache Server, specifies the maximum number of audit actions recorded in the audit log file. The default value is 500. If this maximum number of records is exceeded, the server will open a new log file.

Related Information

Standard options for all servers [page 817]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27.3.6 Job Servers

This section provides the command-line options that are specific to Adaptive Job Servers.

The default path to the server on Windows is **<INSTALLDIR>**\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe.

The default path to the server on UNIX is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM>**/boe_jobsd.

Table 145:

Option	Valid Arguments	Behavior
-dir	**<absolutepath>**	Specify the data directory for the Job Server.
-maxJobs	**<number>**	Set the maximum number of concurrent jobs that the server will handle. The default is five.
-requestJSChildPorts	**<lowerbound-upperbound>**	Specify the range of ports that child processes should use in a firewall environment. For example, 6800-6805 limits child processes to six ports. **Note** For this option to take effect, you must also specify the -requestPort setting.
-report_ProcessExtPath	**<absolutepath>**	Specify the default directory for processing extensions. For details, see the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

Related Information

Standard options for all servers [page 817]

27.3.7 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27.3.8 Report Application Server

This section provides the command-line options that are specific to the Report Application Server.

The default path to the server on Windows is **<INSTALLDIR>**\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe.

The default path to the server on UNIX is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM>**/ras/boe_crystalrasd.

Table 146:

Option	Valid Arguments	Behavior
-ipport	**<port>**	Specify the port number for receiving TCP/IP requests when running in stand-alone mode (outside of the BI platform).
-report_ProcessExtPath	**<absolutepath>**	Specify the default directory for processing extensions. For details, see the *SAP BusinessObjects Business Intelligence platform Administrator Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Valid Arguments	Behavior
`-ProcessAffinityMask`	**`<mask>`**	Use a mask to specify exactly which CPUs that RAS will use when it runs on a multi-processor machine. The mask is in the format `0xffffffff`, where each `f` represents a processor, and the list of processors reads from right to left (that is, the last `f` represents the first processor). For each `f`, substitute either 0 (use of CPU not permitted) or `1` (use of CPU is permitted). For example, if you run the RAS on a 4 processor machine and want it to use the 3rd and 4th processors, use the mask `0x1100`. To use the 2nd and 3rd processors, use `0x0110`. **Note** RAS uses the first permitted processors in the string, up to the maximum specified by your license. If you have a two processor license, `0x1110` has the same effect as `0x0110`. **Note** The default value of the mask is `-1`, which has the same meaning as `0x1111`.

Related Information

Standard options for all servers [page 817]

27.3.9 Web Intelligence Processing Server

This section provides the command-line options that are specific to the Web Intelligence Processing Server.

The default path to the server on Windows is **`<INSTALLDIR>`**`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The default path to the server on UNIX is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<PLATFORM>**/WIReportServer.

Table 147:

Option	Valid Arguments	Behavior
-ConnectionTimeout Minutes	**<minutes>**	Specify the number of minutes before the server will timeout.
-MaxConnections	**<number>**	Specify the maximum number of simultaneous connections that the server allows at one time.
-DocExpressEnable		Enables caching of Web Intelligence documents when the document is being viewed.
-DocExpressRealTime CachingEnable		Enables real time caching of Web Intelligence documents.
-DocExpressCache DurationMinutes	**<minutes>**	Specify the amount of time (in minutes) that content is stored in cache.
-DocExpressMaxCache SizeKB	**<kilobytes>**	Specify the size of the document cache.
-EnableListOfValues Cache		Enables the caching per user sessions of lists of values
-ListOfValuesBatchSize	**<number>**	Specify the maximum number of values that can be returned per list of values batch.
-UniverseMaxCacheSize	**<number>**	Specify the number of universes to be cached.
-WIDMaxCacheSize	**<number>**	Specify the maximum number of Web Intelligence documents that can be stored in cache.

Related Information

Standard options for all servers [page 817]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

27.3.10 Input and Output File Repository Servers

This section provides the command-line options that are specific to the Input and Output File Repository Servers.

The default path to the servers on Windows is **<INSTALLDIR>**\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe

The default path to the program that provides both servers on UNIX is: **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<platform>**/boe_filesd. By default, the Server Intelligence Agent will launch one instance of boe_filesd for the Input File Repository Server and one instance for the Output File Repository Server.

Table 148:

Option	Valid Arguments	Behavior
-rootDir	**<absolutepath>**	Set the root directory for the various subfolders and files that are managed by the server. File paths used to refer to files in the File Repository Server are interpreted relative to this root directory. **Note** All Input File Repository Servers must share the same root directory, and all Output File Repository Servers must share the same root directory (otherwise there is a risk of having inconsistent instances). Additionally, the input root directory must not be the same as the output root directory. It is recommended that you replicate the root directories using a RAID array or an alternative hardware solution.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Option	Valid Arguments	Behavior
-tempDir	**<absolutepath>**	Set the location of the temporary directory that the FRS uses to transfer files. Use this command line option if you want to control the location of the FRS temporary directory, or if the default temporary directory name generated by the FRS exceeds the file system path limit (which will prevent the FRS from starting). **Note** Do not specify an existing directory for this option. The specified directory will be emptied when the FRS starts, and removed when the FRS shuts down. If you use an existing directory, it will be emptied and removed.
-maxidle	**<minutes>**	Specify the number of minutes after which an idle session is cleaned up.
-legacymode		Allow older versions of the SDK, or clients older than the 4.0 release, to fully access the BI platform.

Related Information

Standard options for all servers [page 817]

27.3.11 Event Server

This section provides the command-line options that are specific to the Event Server.

The default path to the server on Windows is **<INSTALLDIR>**\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe.

The default path to the server on Unix is **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<platform>**/boe_eventsd.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 149:

Option	Valid arguments	Behavior
`-cleanup`	**`<minutes>`**	Specify the frequency (in minutes) with which the server cleans up listener proxies. The value represents the amount of time it takes to perform two cleanups. For example, if you specify a value of 10, the proxies will be cleaned up every five minutes.

Related Information

Standard options for all servers [page 817]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

28 Repository Diagnostic Tool

28.1 Overview of the Repository Diagnostic Tool

The Repository Diagnostic Tool (RDT) is a command-line tool that scans, diagnoses, and repairs inconsistencies that may occur between your Central Management Server (CMS) system database and the File Repository Server (FRS) filestore, or inconsistencies that can occur in the metadata of InfoObjects stored in the CMS database.

During normal operations, it is unusual for the CMS system database to have inconsistencies. However, inconsistencies may occur during unexpected events such as disaster recovery, back-up restoration, or network outages. During these events, the CMS system database may be interrupted while performing a task. This can cause inconsistencies with objects in the CMS system database.

The RDT scans the CMS system database and identifies inconsistencies in such objects as reports, users, user groups, folders, servers, universes, universe connections, and other objects.

The RDT scans for two types of inconsistencies.

- Object to file inconsistencies.
  These are inconsistencies that can occur between InfoObjects in the CMS database and the corresponding files in the File Repositories. For example, a file that is stored in the FRS may be missing a corresponding object in the CMS system database.
- InfoObject metadata inconsistencies.
  These are inconsistencies that may exist in an InfoObject's object definition (metadata) in the CMS database. For example, an InfoObject may reference another InfoObject that does not exist in the CMS database.

The RDT performs two functions, depending on the parameters that you provide when you run the tool:

- It scans the CMS system database and FRS filestore, reports inconsistencies, and outputs a log file in XML format with suggested actions to repair the inconsistencies.
- It scans and repairs the inconsistencies identified in the CMS system database and FRS, and outputs the actions taken to a log file in XML format.

28.2 Using the Repository Diagnostic Tool

The Repository Diagnostic Tool (RDT) is available on any machine with a Central Configuration Manager (CCM) installed on it. This command-line tool scans, diagnoses, and repairs inconsistencies that may occur between the Central Management Server (CMS) system database and the File Repository Server (FRS) filestore, or inconsistencies that may occur in an InfoObject's metadata.

It is recommended that you back up your CMS database and FRS filestore, and run the RDT against the backed-up version while your BI platform services are down. If this is not possible, the RDT can be run on an active database.

If you want to run the RDT on an active database, keep the following considerations in mind:

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

- The RDT will use one database connection while it runs.
- The RDT will only check the consistency of the database to the point in time where it started running. Any inconsistencies that occur while the RDT is running will not be logged or fixed.
- It is recommended that the host machine running the RDT have memory above the normal system recommendations available for processing RDT transactions:
  - A database of 50,000 InfoObjects or fewer should have an additional 350 MB available for processing
  - A database of 50,000 to 400,000 InfoObjects should have an additional 1.7 GB available for processing
  - A database of 400,000 to 1,000,000 InfoObjects should have an additional 4 GB available for processing
- The RDT does not have to be run from your CMS server. Running it on a separate machine can help reduce any impact on system performance.
- The tool may have a moderate impact on database performance while being run.

The RDT does not require the CMS service to be running; the RDT runs directly against the CMS database.

28.2.1 To use the Repository Diagnostic Tool

1. If you are running the tool on a Windows computer, open a command window and run the following command.
   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe <arguments>`, where **<arguments>** is the list of parameters that you want to specify.
2. If you are running the tool on a Unix computer, open a /usr/bin/sh compatible shell, and run the following command.
   `.<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>` where **<platform>** is either "linux_x64", "solaris_sparcv9", "hpux_ia64", or "aix_rs6000_64", and **<arguments>** is the list of parameters that you want to specify.

   > **Note**
   >
   > When entering Unix command-line parameters, you may need to escape or multiply escape special shell characters. For example, if the exclamation mark "!" is used in a password, you may need to escape the exclamation mark, like this: `./ccm.sh -display -username Administrator -password Abc\! defgh123 -cms cmsname`.

The Repository Diagnostic Tool scans your repository for inconsistencies. Depending on the parameters that you specify, it either diagnoses and logs inconsistencies, or it repairs inconsistencies and logs the action that it takes.

`Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` lists the inconsistencies that the tool finds. If you had the tool repair the discrepancies that it finds, it also creates the file `Repo_Repair_yyyy_mm_dd_hh_mm_ss.xml`. This file details which objects are repaired and any orphaned files that were deleted. If there are inconsistencies that could not be repaired these will also be listed.

The path to the log files can be specified by the outputdir parameter. If this parameter is not specified, the default directory for the log files is **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\reposcan` on Windows, and `./sap_bobj/enterprise_xi40/reposcan` on Unix.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> The application also provides a default XSL file that is used with the XML file to produce an HTML page. The XSL file is stored in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` on Windows, and `./sap_bobj/enterprisexi_40/reposcan` on Unix

For a list of the warning messages and recommended actions that the RDT takes when it finds inconsistencies, see *Inconsistencies in the CMS metadata* and *Inconsistencies between the CMS and the FRS* .

Related Information

Inconsistencies in the CMS metadata [page 837]
Inconsistencies between the CMS and the FRS [page 836]

28.2.2 Repository Diagnostic Tool Parameters

The RDT accepts the parameters in the following table:

> **Note**
>
> Command-line arguments override any parameter file entries while executing.

Table 150: General Parameters

Parameter	Optional or Mandatory	Description
dbdriver	Mandatory	The type of driver used to connect to the CMS database. Accepted values are: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `sqlanywheredatabasesubsystem`
connect	Mandatory	The connection details that are used to connect to the CMS database. For example: `-connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"`

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Optional or Mandatory	Description
dbkey	Mandatory	Enter the cluster key for your BI platform deployment. If you do not know the cluster key, reset the cluster key by following these steps: **Note** If the machine is in a cluster, these steps will have to be done for all cluster members. Back up the CMS database and filestore before proceeding. 1. Launch the Central Configuration Manager (CCM). 2. In the CCM, right-click the Server Intelligence Agent (SIA) and choose *Stop*. Do not proceed to Step 3 until the SIA status is "Stopped". 3. Right-click the SIA and choose *Properties*. 4. On the Configuration tab, click *Change* next to *CMS Cluster Key Configuration*. 5. A warning message is displayed. Click Yes to continue. 6. In the *Change Cluster Key* dialog box, enter the same eight-character key in both the *New Cluster Key* and *Confirm New Cluster Key* fields. **Note** The RDT will not run if the dbkey parameter is omitted, or if the cluster key is incorrect. **Note** The cluster key displayed in the CCM is encrypted, and cannot be used in the dbkey parameter. For more information on cluster keys see "Securing the BI Platform" in the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
inputfrsdir	Mandatory	The file path of the Input File Repository Server. **Note** The user account you are logged on with is used to execute the command-line tool. It must have full control to the file location.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Optional or Mandatory	Description
outputfrsdir	Mandatory	The file path of the Output File Repository Server. **Note** The user account you are logged on with is used to execute the command-line tool. It must have full control to the file location.
outputdir	Optional	The file path where the RDT writes the log files. The default value is **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\reposcan on Windows, and ./sap_bobj/enterprise_xi40/reposcan on Unix.
count	Optional	The number of approximate errors to scan. This helps ensure optimum performance. The upper count is 2e31 - 1. A value of 0 is interpreted as the entire repository. The default value is 0.
repair	Optional	Tells the RDT to repair all inconsistencies it may find. The default behavior is to only report inconsistencies but not to perform any repairs. If the -repair parameter exists on the command line, the RDT reports and repairs all inconsistencies. **Caution** This process will delete any orphaned objects or files in the repository database.
scanfrs	Optional	Specifies whether the RDT scans the CMS and FRS for inconsistencies. Acceptable values are **True** and **False**. The default value is **True**.
scancms	Optional	Specifies whether the RDT scans the CMS for inconsistencies between InfoObjects. Acceptable values are **True** and **False**. The default value is **True**.
submitterid	Optional	Specifies the User ID to replace missing or invalid IDs for scheduled objects. If no value is provided, the RDT does not replace the invalid IDs. If the provided User ID doesn't exist in the CMS, the RDT prompts for a valid ID. This parameter is only used when the RDT operates in repair mode.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Optional or Mandatory	Description
startid	Optional	Specifies the object in the CMS database to start the scan for. For example, if you've already scanned the first 500 objects in your repository, you can set **-startid=501** to start a new scan at the 501st object. The default value is **1**.
optionsfile	Optional	Specifies the file path to a parameter file. The parameter file is a text file that lists each command-line option and its values. The file should have one parameter per line. **Note** With this option, you can set all parameters in a Text file as described above. Use this option to point to the parameter file without entering the parameters on the command-line.
syscopy	Optional	This parameter is used when you copy the repository database. You must run the tool on the newly created copy, which will update the copy to prevent it from clustering with the source system servers. If the copy will not be able to communicate with the source system, this is not necessary. It should only be used with the mandatory parameters and not be combined with other optional parameters in this list. **Note** Be careful not to run the RDT with the syscopy parameter on your source system.
trace	Optional	This parameter generates traces (recordings of events that occur during the operation of a monitored component) and collects them in log files with the .glf extension at the location: `<SAP_BOBJ_INST_DIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging`

The following parameters are used if the Repository Diagnostic Tool is running on an active clustered CMS.

Table 151: Using the RDT against a clustered CMS

Parameter	Optional or Mandatory	Description
requestport	Optional	The port number that the RDT uses to communicate to the CMS. Accepts whole, positive numbers. By default, the tool uses the value from the operating system of the machine that the RDT is running on.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Parameter	Optional or Mandatory	Description
numericip	Optional	Whether the RDT uses the numeric IP address instead of the hostname for communication between the CMS and the machine that the RDT is running on. Acceptable values are **True** and **False**. The default value is **False**.
ipv6	Optional	The ipv6 name of the machine that the RDT is running on. Accepts a string. The default value is the hostname of the machine that the RDT is running on.
port	Optional	The ipv4 name of the machine that the RDT is running on. Accepts a string. The default value is the hostname of the machine that the RDT is running on.
threads	Optional	The number of threads to use. Accepts whole, positive numbers. The default value is **12**.

The following parameters are used when the RDT uses SSL to communicate with the CMS database that it scans.

Table 152: Using the RDT with SSL

Parameter	Optional or Mandatory	Description
protocol	Optional	Specifies whether the tool should run in SSL mode. The only accepted value is **ssl**.
ssl_certdir	Optional	The directory that contains the SSL certificates.
ssl_trustedcertificate	Optional	The file name of the certificate.
ssl_mycertificate	Optional	The file name of the signed certificate.
ssl_mykey	Optional	The file name of the file that contains the private SSL key.
ssl_mykey_passphrase	Optional	The file name of the file that contains SSL passphrase.

Example

The following Windows example scans the CMS and FRS for both kinds of inconsistencies, and repairs the inconsistencies that it finds.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect "UID=root;PWD=<Password1>;DSN=<myDsn>;HOSTNAME=<myHostname>;PORT=<3306>"
```


© 2015 SAP SE or an SAP affiliate company. All rights reserved.

```
-inputfrsdir "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Input"
-outputfrsdir    "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Output"
-dbkey <cluster key>
-repair
```

Example

Unix example:

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

28.3 Inconsistencies between the CMS and the FRS

The following table describes the inconsistencies that may exist between a Central Management Server (CMS) database and the File Repository Servers (FRS) that are recognized by the Repository Diagnostic Tool (RDT).

- Warning Message
  The warning message that is written to the scan and repair log files.
- Inconsistency
  An explanation of the inconsistency that the RDT finds for the object.
- Suggestion
  The action that the RDT suggests when it finds an inconsistency. This is found in the scan log file.
- Action
  The action that the RDT takes to repair an inconsistency. This is found in the repair log file.

Warning Message	Inconsistency	Suggestion	Action
<Object Name> object **<Object Type>** (Object ID = **<ID>**) is referencing files that do not exist in the FRS (**<File Name>**).	The object exists in the CMS database, but there is no corresponding file in the FRS.	Allow the application to delete this object. Any objects that are descendants of this object will also be deleted.	Deleted this object from the repository.
File **<File Name>** exists in the Input or Output FRS, but there is no corresponding InfoObject in the repository.	The file exists in the FRS, but there is no corresponding file in the CMS database.	Allow the application to remove the unlinked file.	No action taken.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**) has file **<File Name>**. The stored file size is **<Size>** bytes which does not match	The size of the file does not match the InfoObject file size.	Allow the application to update the object with the correct file size.	Updated the object to have the correct file size.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Warning Message	Inconsistency	Suggestion	Action
the actual file size **<Size>** bytes.			
This directory contains no files.	The FRS folder is empty.	Allow the application to remove the directory.	Removed the empty folder.

28.4 Inconsistencies in the CMS metadata

The following table describes the inconsistencies that can occur in the metadata of the objects that are in a Central Management Server (CMS) system database, that are recognized by the Repository Diagnostic Tool (RDT).

- Warning Message
  The warning message that is written to the scan and repair log files.
- Inconsistency
  An explanation of the inconsistency that the RDT finds for the object.
- Suggestion
  The action that the RDT suggests when it finds an inconsistency. This is found in the scan log file.
- Action
  The action that the RDT takes to repair an inconsistency. This is found in the repair log file.

Warning Message	Inconsistency	Suggestion	Action
<Object Type> Object **<Object Name>** (Object ID = **<ID>**)'s parent object is missing (Parent Object ID = **<ID>**).	The object has a missing or invalid Parent Object ID.	Allow the application to move the object to the "BOE Repair" folder.	Moved the object and its children objects to the BOE Repair folder.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**) owner object is missing (Owner Object ID = **<ID>**).	The object has a missing or invalid Owner Object ID.	Allow the application to assign the object to the Administrator.	Assigned the object to the Administrator.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**) submitter object is missing (Submitter Object ID = **<ID>**).	The object has a missing or invalid Submitter Object ID.	The recommendation that the RDT displays depends on whether you've provided a value for the -submitterid parameter. • If you provide this parameter, the recommendation is "Allow the application to update the object with	If you provide a value for the -submitterid parameter, the RDT applies the value for the object's submitter ID. If you don't provide a value for this parameter, the RDT takes no action. When you reschedule the object, the CMS applies a new ID.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Warning Message	Inconsistency	Suggestion	Action
		the provided submitter ID". • If you don't provide this parameter, the recommendation is "Reschedule the object or use the -submitterid command line to replace the invalid submitter ID."	
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**) property of last successful instance refers to a missing object (Last Successful Instance Object ID = **<ID>**).	The object's last successful instance is missing or invalid.	Allow the application to recalculate the property.	Recalculated the property.
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**)'s calendar object is missing (Calendar Object ID = **<ID>**).	The object references a calendar that doesn't exist.	Reschedule the object with an existing calendar. No action can be taken by this application.	No action taken.
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**)'s required scheduling server group is missing (Server Group Object ID = **<ID>**).	The preferred server does not exist.	Reschedule the object and choose an existing server group. No action can be taken by this application.	No action taken.
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**)'s list of pending events contains missing object(s) (Event Object ID(s) = **<ID>**).	The event or events that this object is waiting on does not exist.	Reschedule the object to wait for existing event objects. No action can be taken by this application.	No action taken.
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**)'s list of events to trigger contains missing object(s) (Event Object ID(s) = **<ID>**).	This object triggers an event that does not exist.	Allow the application to remove missing events from the object's list of events to trigger.	Removed the missing events from the object's list of events to trigger.
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**)'s Access Control list references a missing principal (Principal Object ID = **<ID>**).	Orphaned Access Control entry.	Allow the application to remove the missing principal from the object's Access Control list.	Removed the missing principal from the object's Access Control list.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Warning Message	Inconsistency	Suggestion	Action
<Object Type> Object '**<Object Name>**' (Object ID = **<ID>**)'s Access Control list references a missing access level (Access Level Object ID = **<ID>**).	Orphaned Access Control entry.	Allow the application to remove the missing access level from the object's Access Control list.	Removed the missing access level from the object's Access Control list.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**) has multiple Favorites folders.	A specific user account has multiple favorites folders.	Allow the application to consolidate multiple folders into a single Favorites folder.	All Favorites folders have been consolidated into a single Favorites folder.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**) contains invalid Input File entries (**<Files>**).	The object contains invalid entries in its Input Files list.	Allow the tool to remove the object's invalid entries from its Input Files list.	Removed the invalid entries from the object's Input Files list.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**) contains invalid Output File entries (**<Files>**).	The object contains invalid entries in its Output Files list.	Allow the tool to remove the object's invalid entries from its Output Files list.	Removed the invalid entries from the object's Output Files list.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**)'s required caching server group is missing (Server Group Object ID = **<ID>**).	The object is missing the required caching server group.	Reschedule the object and choose an existing server group.	No action taken.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**)'s required processing server group is missing (Server Group Object ID = **<ID>**).	The object is missing the required processing server group.	Reschedule the object and choose an existing server group.	No action taken.
<Object Type> Object **<Object Name>** (Object ID = **<ID>**)'s list of profiles contains missing object(s) (Profile Object ID(s) = **<ID>**).	The object contains missing objects in its list of profiles.	Please update your Publication with existing profiles. No action can be taken by the application.	No action taken.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

29 Rights Appendix

29.1 About the rights appendix

This rights appendix lists and describes most rights that can be set on different objects in the BI platform system. In cases where you require more than one right to perform a task on an object, it also provides information about the additional rights that you require and which objects you must have those rights on. For more information about setting rights see the *Setting Rights* chapter in the *SAP BI platform Administrator Guide*.

29.2 General rights

The rights in this section apply to multiple object types. Many of these rights also have equivalent owner rights. Owner rights are rights that apply only to the owner of the object on which the rights are being checked.

The following rights apply only to objects that can be scheduled:

- The *Schedule the document to run* right.
- The *Schedule on behalf of other users* right.
- The *Schedule to destinations* right.
- The *View document instances* right.
- The *Delete instances* right.
- The *Pause and resume document instances* right.
- The *Reschedule instances* right.

Right	Description
View objects	Lets you view objects and their properties. If you do not have this right on an object, the object is hidden in the BI platform system. This right is a basic right that is required for all tasks.
Add objects to the folder	Lets you add objects to a folder. This right also applies to objects that behave like folders such as inboxes, `Favorites` folders, or object packages.
Edit objects	Lets you edit object content and the properties for objects and folders.
Modify the rights users have to objects	Lets you modify security settings for an object.
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

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	on the user and the object itself. For more information about this right, see the "Setting Rights" chapter of the *SAP BusinessObjects Business Intelligence Platform Administrator Guide*.
Define server groups to process jobs	Lets you specify which server group to use when objects are processed. This right only applies to objects for which you can specify processing servers. To specify a server group, you also require the *Edit objects* right on the object.
Delete objects	Lets you delete objects and their instances.
Copy objects to another folder	Lets you create copies of objects in other folders in the CMS. To do this, you also require the *Add objects to the folder* right on the destination folder. **Note** When an object is copied, the explicit security on the object is not copied; the new object inherits security settings from the destination folder, but you must reset explicit security.
Replicate content	Lets you replicate objects to another system in a federated deployment.
Schedule the document to run	Lets you schedule objects.
Schedule on behalf of other users	Lets you schedule objects for other users or groups. The user or group that you schedule the object for becomes the owner of the object instance. To schedule an object for other users or groups, you also require the following rights: • This right on the user or group. • The *Schedule the document to run* right on the object.
Schedule to destinations	Lets you do the following: • Schedule objects to destinations other than the default Enterprise location. • Modify the default destinations specified for scheduling. To schedule the object to destinations, you also require the following rights: • The *Schedule the document to run* right on the object that you want to schedule.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	• The *Add objects to the folder* right on the recipient inbox (if you want to schedule to an inbox destination). • The *Copy objects to another folder* right on the object that you want to schedule (if you want to send a copy to an inbox destination instead of a shortcut).
View document instances	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 Information

Owner rights [page 136]
Choosing between Modify the rights users have to objects options [page 135]

29.3 Rights for specific object types

29.3.1 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).

Related Information

Type-specific rights [page 118]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

29.3.2 Categories

The rights in this section are general rights that have a specific meaning in the context of public and personal categories.

> **Note**
>
> Objects in categories do not inherit rights that are set on the categories.

Right	Description
Add objects to the folder	Lets you create new categories within categories. This right is not needed to add objects to a category.
Edit objects	Lets you do the following: • Modify category properties. • Move the category into another category as a sub-category. • Add objects to the category. • Remove objects from the category. To move a category into another category as a sub-category, you also require the following rights: • The *Delete objects* right on the original category. • The *Add objects to the folder* right on the destination category.
Delete objects	Lets you delete the category.

29.3.3 Desktop Intelligence documents

The rights in this section apply to Desktop Intelligence documents only.

Right	Description
Use Lists of Values	Allows the users to use lists of values.
Download file associated with the object	Allows the users to download file associated with the object.
Export the report's data	Allows the users to export document data to Excel, PDF, and CSV formats. If you do not have this right, you require the *Save as CSV*, *Save as Excel*, or *Save as PDF* right; these rights let you export documents in the specified format only.
View SQL	Allows the users to see the SQL generated for the query.
Refresh the report's data	Allows the users to refresh document data.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Refresh List of Values	Allows the users to refresh lists of values for prompts when you create the prompt or when you view the document. To do this, you also require the *Use Lists of Values* right on the document.

The document rights specific to PDF, XLS, Rich text, Text:

Right	Description
Add objects to the folder	Allows the users to add objects to a folder. This right also applies to objects that behave like folders such as inboxes, favorites folders, or object packages.
Copy objects to another folder	Allows the users to 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.
Delete instances	Allows the users to delete object instances only. If you have the "Delete objects" right, you do not require this right to delete instances.
Delete objects	Allows the users to delete this category.
Edit objects	Allows the users to modify category properties, move the category into another category as a sub-category, add objects to the category, remove objects from the category.
Modify the rights users have to objects	Allows the users to modify any right, for any user on that object.
Pause and resume document instances	Allows the users to pause or resume object instances that are running.
Replicate content	Allows the users to replicate objects to another system in a federated deployment.
Reschedule instances	Allows the users to reschedule object instances.
Securely modify rights users have to objects	Allows the users to grant, deny or revert to unspecified only the rights he is already granted.
View document instances	Allows the users to view object instances. This right is a basic right that is required for all tasks that you perform on object instances.
View objects	Allows the users to see the category and the sub-categories it contains.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

29.3.4 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	This right lets you do the following: • Start and reply to discussion threads. • View notes on a discussion thread. • Modify or delete notes that you posted.

29.3.5 Crystal reports

The rights in this section apply to Crystal reports only.

> **Note**
>
> These rights only apply when Crystal reports are in the BI platform environment. When you download Crystal reports to your local disk, these rights are ineffective. To prevent this, you can deny the *Download files associated with the object* right on the Crystal report.

Right	Description
Print the report's data	Lets you print the report.
Refresh the report's data	Lets you refresh report data.
Export the report's data	Lets you export report data to any format when you view the report online in the Crystal Reports viewer. To export report data in RPT format, you also require the *Download files associated with the object* right.
Download the files associated with the object	This right lets you do the following: • Export the report in RPT format. • Open the report in Crystal Reports Designer. • Schedule the report in RPT format to external destinations.

29.3.6 Web Intelligence documents

The rights in this section apply to Web Intelligence documents only.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Use Lists of Values	Lets you use lists of values.
Export the report's data	Lets you export document data to Excel, PDF, and CSV formats. If you do not have this right, you require the *Save as CSV*, *Save as Excel*, or *Save as PDF* right; these rights let you export documents in the specified format only.
Query script - enable viewing (SQL , MDX...)	Lets you view query scripts (SQL and MDX).
Refresh the report's data	Lets you refresh document data.
Edit Query	Lets you edit queries in the document.
Refresh List of Values	Lets you refresh lists of values for prompts when you create the prompt or when you view the document. To do this, you also require the *Use Lists of Values* right on the document.
Save as CSV	Lets you export documents as CSV files only. If you have the *Export the report's data* right on a document already, you do not require this right.
Save as Excel	Lets you export documents as Excel files only. If you have the *Export the report's data* right on a document already, you do not require this right.
Save as PDF	Lets you export documents as PDF files only. If you have the *Export the report's data* right on a document already, you do not require this right.
Send to	Lets you send documents to the Scheduler, to a BI platform Inbox, or to send as hyperlinks in email. This right also lets Web Intelligence Rich Client users send documents as email attachments.

29.3.7 Users and groups

You can set rights on users and groups as you would on other objects in the BI platform environment. The rights in this section are type-specific rights that apply to user and group objects only or general rights that have a specific meaning in the context of users and groups.

> **Note**
>
> Users and subgroups can inherit rights from group membership.

> **Note**
>
> The creator of a user account is considered 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.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Edit objects	Lets you do the following: • Edit properties for the user or group. • Manage group membership. To add a user or group to another group, you require this right on the user or group and on the destination group.
Change user password	Lets you do the following: • Change the password for your user account. To do this, you also require the *Edit objects* right on your user account. • Change the password for another user's account. To do this, you also require the *Edit objects* right and the *Modify the rights users have to objects* right on the user account. **Note** This right does not affect the following user password settings: *Password never expires* *User must change password at next logon* *User cannot change password* **Note** This right does not apply to data source credentials for SAP BusinessObjects Universes.
Subscribe to publications	Lets you add the user to publications as a recipient.
Schedule on behalf of other users	Lets you schedule objects on behalf of the user so that the user becomes the owner of the object instance. To do this, you also require the *Schedule on behalf of other users* right on the object.
Add or edit user attributes	Lets you change the value of a user's email address or custom user attributes. This right is applicable to users.
Add or edit user attributes (owner right)	Lets the owner of a user object change the value of the user's email address or custom user attributes. This right is applicable to users.

29.3.8 Access levels

The rights in this section apply to access levels only.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 Information

Choosing between Modify the rights users have to objects options [page 135]

29.3.9 Universe (.unv) rights

The rights in this section apply to universes created with the universe design tool, or .unv universes. The rights listed are type-specific rights that apply to universes only, or general rights that have a specific meaning in the context of universes.

> **Note**
>
> Universe rights apply only when you import universes from the CMS in the universe design tool application. These rights do not apply when the universe is saved to local disk.

Right	Description
Add objects to the folder	Lets you add restriction sets or objects to the universe. To do this, you also require the *Edit Access Restrictions* right.
View objects	Lets you access and view the universe.
Edit objects	This right lets you do the following: • Edit the universe in the CMC or in the universe design tool. • Lock or unlock the universe. To unlock a universe, you also require the *Unlock Universe* right.
Delete objects	Lets you delete the universe.
Translate objects	Lets you to save translated universe object names using the translation management tool.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	Note You can also save translations if you have the *Edit objects* right explicitly granted as long as the *Translate objects* right is not explicitly denied.
New List of Values	This right lets you do the following: • Associate new lists of values with objects. • Edit existing lists of values. **Note** This right does not prevent you from creating cascading lists of values.
Print Universe	Lets you print the universe.
Show Table or Object Values	Lets you see the values associated with tables or objects in the universe.
Edit Access Restrictions	Lets you edit access restrictions (overloads) for the universe.
Unlock Universe	Lets you do the following: • Unlock the universe if it is locked by another user. • Export the universe from the CMS. To unlock a universe, you also require the *Edit objects* right.
Data Access	Lets you retrieve data from the universe and refresh documents based on the universe. To do this, you also require this right on the universe design tool application, the document, and the universe connection.
Create and Edit Query based on the universe	Lets you create documents and edit queries that are based on the universe.

29.3.10 Universe (.unx) rights

The rights in this section apply to universes created with the information design tool, or .unx universes. The rights listed are type-specific rights that apply to universes only, or general rights that have a specific meaning in the context of universes.

Note

Universe rights apply only to universes published to a repository. These rights do not apply when the universe is saved to a local folder.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
View objects	Lets you access and view the universe.
Edit objects	Lets you to republish the universe.
Delete objects	Lets you delete the universe.
Retrieve universe	Lets you to retrieve a published universe and edit the underlying resources (business layer and data foundation) in the information design tool. **Note** You must also have the information design tool application right *Retrieve universes* granted.
Edit security profiles	Lets you to insert, edit, and delete security profiles for the universe in the information design tool security editor. **Note** This right is not required to view security profiles or to change security profile aggregation options.
Assign security profiles	Lets you to assign and unassign security profiles to users and groups in the information design tool security editor.
Data Access	Lets you retrieve data from the universe and refresh documents based on the universe. In the information design tool, this right lets you to preview the result set in the query panel.
Create and edit queries based on this universe	Lets you create and edit queries that are based on the universe. In the information design tool, this right lets you open the query panel and run a query on the universe.
Save for all users	Lets you save the universe for all users. **Note** You must also have the information design tool application right *Save for all users* granted.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

29.3.11 Universe object-access levels

When designers create a universe using the universe design tool, or a business layer using the information design tool, they assign an object-access level to every object in the universe. The object-access levels are:

Public (default)
Controlled
Restricted
Confidential
Private

Once the universe is published in the repository, you can grant access to universe objects based on the object-access levels assigned in the application. For example, you can grant Public access to the Everyone group. This allows users in the Everyone group to see the objects in the universe designated as Public.

Each object-access level grants more access to objects than the previous one. Public is the lowest level. Principals granted Public access can only see objects designated as Public. Principals granted Controlled access can see objects designated as Public and Controlled. Private is the highest level setting and grants principals access to all object-access levels, in other words, all objects in the universe.

> **Note**
>
> Object-access level security settings override any security settings that the universe inherits.

> **Note**
>
> For .unx universes, object-access level security settings are taken into consideration with the object security defined by the security profile. For more information on security profiles, see the *Information Design Tool User Guide*.

Related Information

Assigning universe object-access levels [page 851]

29.3.11.1 Assigning universe object-access levels

To set universe object-access level security, you require the *Modify the rights users have to objects* right on the universe.

1. In the *Universes* area of the CMS, select the universe.
2. Click *Action* > *Universe Security*.
3. In the *Universe Security* dialog box, for the user or group, select the object-access level in the *Object Level Security* list.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

29.3.12 Connection rights

The rights in this section are type-specific rights that apply to universe connections or general rights that have a specific meaning in the context of universe connections. These rights apply to connections published in the repository.

Relational connection rights

Right	Description
View objects	Lets you view the connection.
Edit objects	Lets you edit the connection parameters.
Download connection locally	Lets you use universes created on the connection in Web Intelligence Rich Client in offline mode. Lets you use the local middleware driver in the information design tool. To do so, select the local middleware option in the information design tool preferences, otherwise queries to the database will use the server middleware. This right is also needed to edit a secured connection in the information design tool.
Delete objects	Lets you delete the connection.
Copy objects to another folder	Lets you copy the connection from one folder to another.
Data Access	Lets you retrieve content from the database specified in the connection. In the information design tool, this right lets you browse table data from the connection and data foundation editors. It also lets you preview the result set in the query panel.
Use connection for Stored Procedures	Lets you use the stored procedures in the database specified for the universe connection. **Note** This right applies to .unv universes only.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

OLAP connection rights

Right	Description
View objects	Lets you view the connection.
Edit objects	Lets you edit the connection parameters in the information design tool connection editor.
Delete objects	Lets you delete the connection.
Copy objects to another folder	Lets you copy the connection from one folder to another.

29.3.13 Applications

29.3.13.1 CMC

Right	Description
Log on to the CMC and view this object in the CMC	Enables a user to log on to the CMC
Allow access to Instance Manager	Enables a user to access the Instance Manager
Allow access to Relationship Query	Enables a user to run relationship queries in the CMC
Allow access to Security Query	Enables a user to run security queries in the CMC

29.3.13.2 BI launch pad

Right	Description
Organize	Enables a user to move and copy objects, add objects to the `Favorites` folder, and create shortcuts to objects
Send to Business Objects inbox	Enables a user to send objects to recipient BI Inboxes
Send to email destination	Enables a user to send objects to recipients via email
Send to file location	Enables a user to send objects to a file location
Send to FTP location	Enables a user to send objects to an FTP location
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.2.1 Rights for collaboration applications

These access rights apply to SAP Jam or SAP StreamWork, when the application is configured in the BI platform.

Right	Description
Comment on documents owned by the user	Enables a user to comment on documents and instances that the user owns
View comments on documents owned by the user	Enables a user to view comments on documents and instances that the user owns
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the application.

29.3.13.3 BI workspaces

Right	Description
Create and edit BI workspaces	Enables a user to create new BI workspaces and to edit existing BI workspaces
Create and edit modules	Enables a user to create new modules and to edit existing modules
Edit BI workspaces	Enables a user to edit existing BI workspaces (but does not enable a user to create new workspaces)
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.4 Desktop Intelligence

Right	Description
Create and edit connections	Enables a user to create a new connection and to edit an existing one
Data provider manipulation	Enables a user to modify a query and to change the universe it is based on
Edit free hand SQL	When granted with the *Use Free-hand SQL* right, enables a user to edit a query that uses freehand SQL scripts as a data provider
Use free hand SQL	Enables a user to create a query using freehand SQL scripts as a data provider
Refresh Document list and categories	Enables a user to refresh the document list
Send documents to repository	Enables a user to publish a document in the CMS to the `Public` folder or to `Personal` folders
Send documents to Mail	Enables a user to send documents, attached to an email message, from the Desktop Intelligence application
Retrieve Documents	Enables a user to import a document from the CMS
Run VBA code	Enables a user to run VBA code
Install Add-INS	Enables a user to install or uninstall VBA add-ins
Manage all corporate categories	Enables a user to create, edit, or delete any documents in the category
Manage my corporate categories	Enables a user to create, edit, and delete corporate categories in the Desktop Intelligence application
Edit Scope of Analysis	Enables a user to edit the Scope of Analysis

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Work in drill mode	Enables a user to drill on details in reports
Work in slice and dice mode	Enables a user to use the Slice and Dice panel
Edit VBA code	Enables a user to edit VBA macros in reports
Euro converter	Enables a user to convert currency figures in reports to and from Euros
Copy to clip board	Enables a user to cut and copy document content
Drill through	Enables a user to drill further in a report by retrieving new data
Edit Euro converter rate	Enables a user to modify the Euro exchange rate that is used by the Euro Converter function
Desktop Intelligence report interaction n	Enables a user to cut, copy, clear, duplicate, and delete individual elements in a report
Desktop Intelligence document interaction	Enables a user to rename, duplicate, insert, and delete a report in a document
Print documents	Enables a user to print a document
Refresh Desktop Intelligence content	Enables a user to refresh Desktop Intelligence content
Use templates	Enables a user to create a report with a template and to apply a template to existing content in a report
Create templates	Enables a user to save a document as a template
Save documents for all users	Enables a user to save a document without security constraints for offline use, to enable all users to view the document when it is saved locally
Create Desktop Intelligence documents	Enables a user to create a new document
Save Desktop Intelligence documents	Enables a user to save a document locally
Send documents to inbox	Enables a user to send a document to a BI launch pad Inbox
Use user objects	Enables a user to create, edit, and delete user objects
Refresh list of values	Enables a user to refresh lists of values
Use list of values	Enables a user to use and to refresh lists of values in a document
Edit list of values	Enables a user to edit lists of values defined in a universe

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Use queries	Enables a user to create new queries based on a universe
Edit queries	Enables a user to edit queries based on a universe
View SQL	Enables a user to see the SQL generated for a query
Edit query SQL	Enables a user to modify the SQL generated for a query
Always regenerate SQL	Enables queries to be regenerated with each refresh
Use stored procedures	Enables a user to create a report using a stored procedure as a data provider
Edit stored procedures	Enables a user to edit parameters in stored procedures
Use personal data file	Enables a user to create a report using Excel, dBase, or ASCII text files as a data provider
Edit personal data file	Enables a user to edit the personal data provider
Securely modify rights users have to object	Enables a user to grant, deny, and revert to unspecified granted access rights
Modify the rights users have to this object	Enables a user to modify access rights for any user of a particular object
Edit this object	Enables a user to modify the application's properties in the CMC
Logon to Desktop Intelligence and view this object in CMC	Enables a user to log on to Desktop Intelligence and view the object in the CMC
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

29.3.13.5 Web Intelligence

The access rights in this section apply to the Web Intelligence application, including the Rich Client interface, and can affect viewers and query panels in the application.

Right	Description
Data - enable data tracking	Enables a user to track changed data
Data - enable formatting of changed data	Enables a user to select formatting for changed data
Desktop interface - enable Web Intelligence Desktop	Enables a user to use the Web Intelligence Desktop interface
Desktop interface - export documents	Enables a user to export documents to the CMS in the Web Intelligence Desktop interface
Desktop interface - import documents	Enables a user to import documents from the CMS in the Web Intelligence Desktop interface
Desktop interface - install from BI launch pad	Enables a user to download the Web Intelligence Desktop interface from the BI launch pad
Desktop interface - print documents	Enables a user to print documents from the Web Intelligence Desktop interface
Desktop interface - remove document security	Enables a user to remove document security from the Web Intelligence Desktop interface
Desktop interface - save document for all users	Enables a user to save documents for all users from the Web Intelligence Desktop interface
Desktop interface - save documents locally	Enables a user to save documents to a local disk in the Web Intelligence Desktop interface
Desktop interface - send by mail	Enables a user to send document in an email message from the Web Intelligence Desktop interface
Desktop Interface - enable local data providers	Enables a user to use personal data providers in the Web Intelligence Desktop interface
Documents - disable automatic refresh on open	Prevents documents from automatically refreshing when they are opened
Documents - enable autosave	Enables documents to be automatically saved, if autosaving is activated in the CMC by the administrator
Documents - enable creation	Enables a user to create new documents
Documents - enable publishing and content management	Enables a user to publish document in the CMS
Interactive: Reporting - Create and edit alerter	Enables a user to create and to edit alerts in the interactive viewer

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
s	
Interfaces - enable Rich Internet Application	Enables a user to use the viewing and editing interface in the Rich Internet Application The Rich Internet Application was called Java Report panel in earlier releases.
Interfaces - enable web viewing interface	Enables a user to use the Web viewing interface The Web viewing interface was called the DHTML viewer in earlier releases.
Interfaces - enable web query panel	Enables a user to use of the web query panel The web query panel was called Query - HTML in earlier releases.
General - edit 'My Preferences'	Enables a user to edit preferences in the BI launch pad
General - enable right-click menus	Enables a user to use context menus
Left pane - enable document summary	Enables a user to display the document summary in the left pane
Left pane - enable document structure and filter s	Enables a user to display the document structure and filters in the left pane
Query script - enable editing (SQL, MDX...)	Enables a user to edit SQL and MDX query scripts
Query script - enable viewing (SQL, MDX...)	Enables a user to view SQL and MDX query scripts
Reporting - create and edit breaks	Enables a user to create and to edit breaks
Reporting - create and edit conditional formatting rules	Enables a user to create and to edit conditional formatting rules
Reporting - create and edit predefined calculations	Enables a user to create and to edit predefined calculations
Reporting - create and edit input controls	Enables a user to create and to edit input controls
Reporting - create and edit report filters and consume input controls	Enables a user to creation and editing of report filters and input controls(Input Controls pane in the Left Pane are not displayed when disabled)
Reporting - create and edit sorts	Enables a user to create and to edit sorts
Reporting - create formulas and variables	Enables a user to create formulas and variables

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Reporting - enable formatting	Enables a user to edit report formatting Without this access right, the Design and Data mode is not available.
Reporting - enable merged dimensions	Enables a user to synchronize data using merged dimensions in reports and in the data manager
Reporting - insert and remove reports, tables, charts and cells	• Enables a user to insert and to remove reports, tables, charts, and cells • Enables the duplicates workflow (copy/paste)
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.6 Strategy Builder

These access rights apply to Strategy Builder and can affect goals management in Performance Manager or specific features in Strategy Builder.

Right	Description
Create, Modify, or Delete Goals	Enables a user to add, edit, or remove goals in Performance Manager
View Goals	Enables a user to see goals in analytics
Access to Goal Management	Enables a user to view goals on the *Goals Management* page in Performance Manager
Publish Goals	Enables a user to publish goals in Performance Manager
Access to Strategy Builder	Enables a user to access the Strategy Builder in Performance Manager
Create, Modify, or Delete Roles	Enables a user to administer the roles used to publish goals and metrics for particular audiences in Strategy Builder
Create, Modify, or Delete Strategies	Enables a user to create strategies that link roles and that publish goals and metrics in Strategy Builder
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.7 Universe design tool

Right	Description
Check Universe Integrity	Enables a user to check universe integrity
Refresh Structure Window	Enables a user to refresh the structure window
Use Table Browser	Enables a user to view database data, using the table browser
Apply Universe Constraints	Enables a user to apply predefined universe constraints to users of an imported universe
Link Universe	Enables a user to link two universes and share components
Create, Modify or Delete Connections	Enables a user to create, modify, and delete universe connections that are stored in the BI platform repository or stored as personal or shared connections
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.8 Information design tool

Right	Description
Administer security profiles	Enables a user to open the security editor

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	To work with security profiles, you also need rights granted on the universe.
Share projects	Enables a user to share a local project and to synchronize a shared project with the local project
Create, modify, or delete connections	• Enables a user to create and to delete secured connections from the Published Resources view • Enables a user to edit connections in the connection editor • Enables a user to publish connections to a repository
Publish universes	Enables a user to publish universes to a repository
Retrieve universes	Enables a user to retrieve published universes in a local project that will be edited
Save for all users	Enables a user to save for all users when retrieving universes
Compute statistics	Enables a user to select tables and columns on which to calculate and publish statistics
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.9 Widgets for the BI platform

Right	Description
Use Explorer	Enables a user to use Document List Explorer to browse content on all connected BI platform servers
Use Search	Enables a user to use the Content Search to concurrently search all connected BI platform repositories
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.10 Alerting

Right	Description
Trigger Alerts	Enables a user to trigger alert events. To trigger an alert for a document, the following additional rights are required: • "View" and "Schedule" rights on the document • "View" and "Trigger" rights on the corresponding event
Subscribe to Objects	Enables a user to subscribe to an alert event. To subscribe to an event, the following additional rights are required: • "View" right on the corresponding event • "Subscribe" right on the user's own account To subscribe to an alert in a document, the following additional rights are required: • "View" right on the document • "View Instance" right on the document • "View" right on the corresponding event • "Subscribe" right on the user's own account
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.11 Explorer

Right	Description
Log on to Explorer and view this object in the CMC	Enables a user to log on to Explorer and to view objects in the CMC

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Explore Information Spaces	Enables a user to explore an Information Space. To log on to Explorer, the "Log on to Explorer and view this object in the CMC" right is also required.
Explore Information Spaces: Export to Bookmark/Email	Enables a user to create bookmarks and to email bookmarks, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Explore Information Spaces"
Explore Information Spaces: Export to CSV	Enables a user to export the results of an exploration to a CSV or Excel file, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Explore Information Spaces"
Explore Information Spaces: Export to Image	Enables a user to export the results of an exploration as an image, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Explore Information Spaces"
Explore Information Spaces: Export to Web Intelligence	Enables a user to export the results of an exploration as a query, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Explore Information Spaces"
Manage Information Spaces	Enables a user to access the *Manage Spaces* menu and to perform associated tasks, when combined with the "Log on to Explorer and view this object in the CMC" right
Manage Information Spaces: Create a new Space	Enables a user to create a new Information Space, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Manage Information Spaces"
Manage Information Spaces: Modify a Space	Enables a user to modify or to delete an Information Space, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Manage Information Spaces"
Manage Information Spaces: Schedule indexing	Enables a user to schedule indexing for Information Space data, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Manage Information Spaces"

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
Manage Information Spaces: Launch indexing	Enables a user to run indexing for Information Space data, when combined with the following additional rights: • "Log on to Explorer and view this object in the CMC" • "Manage Information Spaces"
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

29.3.13.12 SAP BusinessObjects Mobile

Right	Description
Log on to SAP BusinessObjects Mobile application	Enables a user to log on to the BI platform from the Mobile application and to view documents
Subscribe to document alerts	Enables a user to subscribe to document and recurring-instance alerts If a user has been granted this right in the past (even if it is no longer granted), the user can still receive subscribed alerts. Users must explicitly unsubscribe to an alert if they do not want to receive it. To subscribe to document alerts and recurring instances for schedules, a user must have "Full Control" access to the `System Events` folder, under *Events* in the CMC.
Save documents to device's localstore	Enables a user to save documents on a mobile device If a user has been granted the "Save documents locally on the device" right in the past (even if it is no longer granted) and has saved documents on the mobile device, the documents still exist on the device, but they are not synchronized during the synchronization process.
Send documents from device as an email	Enables a user to send reports in an email message
Change preferences for objects that the user owns	Displays the *Preferences* menu in an application object

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Right	Description
	Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application.

For more information, see the *SAP BusinessObjects Mobile Installation and Deployment Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

30 Server Properties Appendix

30.1 About the server properties appendix

This server properties appendix lists and describes properties that can be set for each BI platform server.

> **Note**
>
> For information about SAP BusinessObjects Explorer server properties and metrics, see the *SAP BusinessObjects Explorer Administrator's Guide*.

30.1.1 Common Server Properties

The server properties described in this section apply to all server types.

Table 153: Request Port Properties

Property	Description	Default Value
Server Name	The name of the server.	The default value is the name of the node that the server is on plus the name of the server.
ID, CUID	The short ID and cluster unique ID of the server. Read-only.	These values are auto-generated.
Node	The name of the node where the server is located.	This values is specified during installation.
Description	The server's description	The default value is the name of the server.
Command Line Parameters	The command-line parameters for the server.	The default value depends on the type of server.
Request Port	Specifies the port from which the server receives requests. In an environment with firewalls, configure the server to only listen to requests on ports that are open on the firewall. If you are specifying a port for the server, ensure that the port is not already taking by another process. **Note** If *Auto assign* is selected, the server binds to a dynamically allocated port. This means that a random port number is allocated to the server each time the server is restarted.	By default *Auto assign* is set to **TRUE**, and the *Request Port* is empty.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Auto assign	Specifies whether the server binds to a dynamically allocated port whenever the server is restarted. To bind the server to a specific port, set *Auto Assign* to **FALSE** and specify a valid *Request Port*.	The default value is **TRUE**.

Table 154: Auto-Start Properties

Property	Description	Default Value
Automatically start this server when the Server Intelligence Agent starts	Specifies whether the server is automatically started when the Server Intelligence Agent (SIA) starts or restarts. If this value is set to **FALSE** and the SIA starts or restarts, the server remains stopped.	The default value is **TRUE**.

Table 155: Host Identifier Properties

Property	Description	Default Value
Auto assign	Specifies whether the server binds to a network interface that is automatically assigned. If set to **FALSE**, the server binds to a specific network interface. If set to **TRUE**, the server accepts requests on the first available IP Address. On multihomed machines, you can specify a particular network interface to bind to by setting this value to **FALSE** and providing a valid hostname or IP Address.	The default value is **TRUE**.
Hostname	The hostname of the network interface that the server binds to. If a host name is specified, the server accepts requests on all IP Addresses associated with the host name.	By default *Auto assign* is set to **TRUE**, and the *Hostname* is empty.
IP Address	The IP Address of the network interface that the server binds to. Both IPv4 and IPv6 protocols are supported. If an IP Address is specified, the server accepts requests on the IP Address only.	By default *Auto assign* is set to **TRUE**, and the *IP Address* is empty.

Table 156: Configuration Template Properties

Property	Description	Default Value
Use Configuration Template	Specifies whether to use a configuration template.	The default value is **FALSE**.
Restore System Defaults	Specifies whether to restore the original default settings for this server.	The default value is **FALSE**.
Set Configuration Template	Specifies whether to use the current service's settings as a configuration template for all services of the same type. If set to **TRUE**, all services of the same type that you have specified to *Use Configuration Template* are immediately reconfigured to use the settings of the current service.	The default value is **FALSE**.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 157: TraceLog Service Properties

Property	Description	Default Value
Log Level	Specifies the minimum severity of messages that you want to be recorded, and determines how much information is recorded in the server log file. Possible log threshold levels are: • *Unspecified* • *None* • *Low* • *Medium* • *High*	The default value is **`Unspecified`**.

Related Information

Working with configuration templates [page 355]
Trace log levels [page 542]

30.1.2 Core Services properties

The Core services category includes the following servers:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Dashboard Server
- Dashboard Analytics Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Web Application Container Server

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Adaptive Job Server properties

Table 158: General properties

Property	Description	Default Value
Temporary Directory	Specifies the directory where temporary files are created on when necessary. You may encounter performance issues if this directory does not have adequate disk space. For better performance, ensure that this directory is located on a local disk. **Note** You must restart the server for changes to take effect.	%DefaultDataDir%

The Adaptive Job Server can host a number of different services. Each service has the following properties

Table 159: Service properties

Property	Description	Default Value
Maximum Concurrent Jobs	Specifies the number of concurrent independent processes (child processes) that the server allows. You can adjust the maximum number of jobs to suit your reporting environment. The default setting is acceptable for most reporting scenarios. The ideal setting for your reporting environment depends on your hardware configuration, database software, and reporting requirements.	5
Maximum Child Requests	Specifies the number of jobs the child will process before restarting.	100

Adaptive Processing Server properties

Table 160: General properties

Property	Description	Default Value
Service Startup Timeout (seconds)	Specifies the amount of time, in seconds, that the server will wait for services to start. If a service fails to start within the time specified, there are two possible reasons: • The service failed, for example, because a required resource such as a database could not be found, or the service encountered a port conflict. • The service could not start within the specified time, for example, because the system is too slow. To find the reason, check the server log file. If the service could not start within the time specified, consider increasing this value.	1200

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 161: Client Auditing Proxy Service properties

Property	Description	Default Value
No configuration properties		

Table 162: Security Token Service properties

Property	Description	Default Value
No configuration properties		

Table 163: Insight to Action Service properties

Metric	Description	
Maximum Number of Active Connections Per User Session	The maximum number of connections with the SAP server available for a user for a given time. When a user opens a report or dashboard that is RRI capable, a connection with the SAP server will be established to determine the available RRI targets.	20
Maximum Number of Idle Connections Per User Session	The number of idle connections to keep open and re-use for subsequent RRI requests. Increasing this setting will allocate additional system resources.	20
Maximum Connection Wait Time (in seconds)	The amount of time the Insight to Action framework should wait for a response from the SAP Server before timing out (in seconds).	30

Table 164: Publishing Service properties

Property	Description	Default value
Thread Pool Size	Specifies how many scope batch processing threads can run at the same time. If the value of this property is set to "0", the thread pool size is determined using a formula based on the number of CPU cores in the current machine.	0

Table 165: Translation Service properties

Property	Description	Default value
No configuration properties		

Table 166: Monitoring Service properties

Property	Description	Default value
No configuration properties		

Table 167: Platform Search Service properties

Property	Description	Default value
No configuration properties		

Table 168: Publishing Post Processing Service properties

Property	Description	Default value
No configuration properties		

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

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 169: Central Management Service properties

Property	Description	Default Value
Name Server Port	Specifies the port on which the CMS listens to initial name service requests.	6400
System Database Connections Requested	Specifies the number of CMS system database connections that the CMS attempts to establish. If the server cannot establish all of the requested database connection, the CMS continues to function but at a reduced performance, since fewer concurrent requests can be served simultaneously. The CMS will attempt to establish additional connections, until the requested number of connection is established. The CMS's *Established System Database Connections* metric shows the current number of established connections.	14
Auto Reconnect to System Database	Specifies whether the CMS automatically attempts to reestablish a connection to the CMS database in the event of a service disruption. If this value is set to **FALSE**, you are able to check the integrity of the CMS database before resuming operations; you must restart the CMS to reestablish the database connection.	**TRUE**

Table 170: Single Sign-on Service properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection to a datasource is valid before expiring. This applies to Windows AD users running reports that are configured for Windows AD SSO to the datasource.	86400

Event Server properties

Table 171: Event Service properties

Property	Description	Default Value
Event Poll Interval (seconds)	Specifies how often the server polls for a file that triggers an event, in seconds.	10 The range of allowed values is 1 to 1200 seconds.
Cleanup Interval (minutes)	Specifies how often cleanup utility runs, in minutes.	20

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Input File Repository Server properties

Table 172: Input Filestore Service properties

Property	Description	Default Value
File Store Directory	Specifies the directory where file repository objects are stored. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultInputFRSDir/%
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space. To ensure better performance, it is recommended that the *Temporary Directory* is located on the same file system as the *File Store Directory*.	%DefaultInputFRSDir/temp%
Maximum Idle Time (minutes)	Specifies the length of time that the server waits before it closes inactive connections. Setting a value that is too low can cause a user's request to be closed prematurely. Setting a value that is too high can cause excessive consumption of system resources such as processing time and disk space.	10
Maximum Retries for File Access	Specifies the number of times the server tries to access a file.	1

Output File Repository Server properties

Table 173: Output Filestore Service properties

Property	Description	Default Value
File Store Directory	Specifies the directory where file repository objects are stored. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultOutputFRSDir/%
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultOutputFRSDir/temp%

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Maximum Idle Time (minutes)	Specifies the length of time that the server waits before it closes inactive connections. Setting a value that is too low can cause a user's request to be closed prematurely. Setting a value that is too high can cause excessive consumption of system resources such as processing time and disk space.	10
Maximum Retries for File Access	Specifies the number of times the server tries to access a file.	1

Web Application Container Server properties

Table 174: General properties

Property	Description	Default Value
Service Startup Timeout (seconds)	How long the WACS will wait for its hosted services to start before it times out. If the timeout passes, the WACS will not provide services that haven't started yet. On a slower machine, you can consider specifying a larger value. If you specify a value that is too small, and the WACS doesn't start before timing out, restore the default settings of the WACS through the Central Configuration Manager (CCM).	1200

Table 175: TraceLog Service properties

Property	Description	Default Value
Log level	Enables logging and sets the level of severity and detail to None (only critical events logged) Low (startup, shutdown, start and end request messages), Medium (error, warning and most status messages) or High (Nothing excluded. Use for debugging only. CPU usage may increase, impacting performance). The available menu choices are: • *Unspecified* • *None* • *Low* • *Medium* • *High*	Unspecified

Table 176: Business Process BI Service properties

Property	Description	Default value
No configuration properties		

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 177: Query Builder Service properties

Property	Description	Default value
No configuration properties		

Table 178: RESTful Web Service - System Property Configuration properties

Property	Description	Default Value
Show Error Stack	When enabled, the error log includes RESTful web service error messages for debugging purposes. It should not be used otherwise, or when there is a security concern where details of the BI platform are revealed.	Not selected
Default Number of Objects on One Page	The number of entries that will be listed per page. Developers can override this setting with the &pageSize=<m> parameter in the RESTful Web Services SDK.	50
Enterprise Session Token Timeout (minutes)	The expiry time a logon token will remain valid. Beyond this time, a new login token must be generated.	60
Session Pool Size	This is the number of cached sessions to be stored at one time that is used to improve server performance. The session pool caches active RESTful web service sessions so they can be reused when a user sends another request that uses the same logon token in the HTTP request header.	1000
Session Pool Timeout (minutes)	The time in minutes that cached sessions will expire.	2
Enable HTTP Basic Authentication	If this setting is not enabled, RESTful web service requests must use a logon token. When this setting is enabled, users must provide their name and password the first time they make a RESTful web service request. When enabled, the *Default Authentication Scheme for HTTP Basic* drop down menu appears.	Not selected
Default Authentication Scheme for HTTP Basic	When *Enable HTTP Basic Authentication* is checked, one of four authentication types may be selected. Note that names and passwords are transmitted in clear text unless HTTPS options are used. Accepted values are: • *secEnterprise* • *secDAP* • *SAPR3* • *secWinAD*	Blank. However, if *Enable HTTP Basic Authentication* is selected, defaults to *secEnterprise*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 179: RESTful Web Service - Cross-Origin Resource Sharing Configuration properties

Property	Description	Default Value
Allow Origins	This setting is to permit users with CORS-capable browsers access to java-scripted pages that must access multiple domain names. Add each domain name and separate each by a comma. For example, http://origin1.server.com:8080, http://origin2.server.com:8080. By default, browsers are allowed access to all domains (*).	* (an asterisk)
Max Age(minutes)	This is the maximum time that browsers may cache HTTP requests.	1440

Table 180: RESTful Web Service - Trusted Authentication Configuration properties

Property	Description	Default Value
Retrieving Method	This setting is a menu that sets which query method will be used to retrieve trusted authentication logon tokens when using the RESTful web service API `/logon/trusted`. • *HTTP_HEADER* is used for GET queries with the request header accept=application/xml (or application/json). • *QUERY_STRING* is used to add a logon name to the end of a URL query using the RESTful Web Service API, for example /logon/trusted/?user=johndoe. • *COOKIE* is used when the login name is retreived from a web browser cookie. The domain, name, value and path must be stored in the cookie.	**HTTP_HEADER**
User Name Parameter	This is the label used to identify the trusted user for the purposes of retrieving a logon token.	**X-SAP-TRUSTED-USER**

Table 181: BOE Web Application Service properties

Property Type	Description	Default Value
Authentication Type	The authentication type that is used to authenticate users logging on to BI launch pad. Accepted values are: • *AD Kerberos* • *AD Kerberos SSO* • *Enterprise* • *LDAP*	*Enterprise*
Default AD Domain	The default Active Directory domain is used so that users do not have to supply a domain when they log in. For example, if the default domain is set to “mydomain” and a user logs on with the username “user”, the Active Directory logon authority tries to authenticate “user@mydomain.com”.	Blank
Service Principal Name	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	Blank
Keytab File	The full path to a keytab file. A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	Blank

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 182: Web Services SDK and QaaWS properties

Property	Description	Default Value
Enable Kerberos Active Directory Single Sign On	Whether to enable Kerberos AD Single Sign-on for Web Services SDK and QaaWS.	**FALSE**
Default AD Domain	The default Active Directory domain is used so that users do not have to supply a domain when they log in.	Blank
Service Principal Name	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	Blank
Keytab File	The full path to a keytab file. A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	Blank

Table 183: HTTP configuration properties

Property	Description	Default Value
Bind to All IP Addresses	Whether to bind to all network interfaces or not. If your server has more than one NIC, and you want to bind to a specific network interface, uncheck this property.	**TRUE**
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTP service is provided. You can only specify a value if you uncheck *Bind to All IP Addresses*.	**localhost**
HTTP Port	The port on which HTTP service is provided.	6405 The range of allowed values is 1 to 65535.
Maximum HTTP Header Size	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

Table 184: Configuration of HTTP through proxy properties

Property	Description	Default Value
Enable HTTP through Proxy	Whether to enable the HTTP through Proxy connector on the WACS. This is typically checked in deployments with a reverse proxy.	**FALSE**
Bind to All IP Addresses	Whether to bind the HTTP through proxy port to all network interfaces or not.	**TRUE**
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTP through Proxy service is provided. You can only specify a value if you uncheck *Bind to All IP Addresses*.	**localhost**
HTTP Port	The port on which HTTP service in a reverse proxy deployment is provided. You can only specify a value if you check *Enable HTTP through Proxy*.	6406 The range of allowed values is 1 to 65535.
Proxy Hostname	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can only specify a value if you check *Enable HTTP through Proxy*.	Blank

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Proxy Port	The port of your forward or reverse proxy server. You can only specify a value if you check *Enable HTTP through Proxy*.	0 The range of allowed values is 1 to 65535.
Maximum HTTP Header Size	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

Table 185: HTTPS configuration properties

Property	Description	Default Value
Enable HTTPS	Whether to enable HTTPS/SSL communication.	`FALSE`
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTPS service is provided. You can only specify a value if you check *Enable HTTPS*.	`localhost`
HTTPS Port	The port on which HTTPS service is provided. You can only specify a value if you check *Enable HTTPS*.	443 The range of allowed values is 1 to 65535.
Proxy Hostname	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can only specify a value if you check *Enable HTTPS*.	Blank
Proxy Port	The port of your forward or reverse proxy server. You can only specify a value if you check *Enable HTTPS*.	0 The allowed range of values is 1 to 65535.
Protocol	The encryption protocol to use. You can only specify a value if you check *Enable HTTPS*.	TLS Allowed values are TLS or SSL.
Certificate Store Type	The type of certificate store that contains your certificates and private keys. In most cases, this will be *PCKS12*. You can only specify a value if you check *Enable HTTPS*.	PKCS12 Allowed values are PKCS12 or JKS.
Certificate Store File Location	The full path to the certificate file. You can only specify a value if you check *Enable HTTPS*.	Blank
Private Key Access Password	PKCS12 certificate stores and JKS keystores have private keys that are password protected, to prevent unauthorized access or theft. Enter the password that you specified when you generated the certificate store here, so that WACS can access private keys from the certificate store. You can only specify a value if you check *Enable HTTPS*.	Blank
Certificate Alias	The alias of the certificate inside the certificate store. If this is not specified, and a certificate store that contains more than one certificate is used, the first certificate in the store is used. In most cases, you do not need to specify a value. You can only specify a value if you check *Enable HTTPS*.	Blank

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Enable Client Authentication	If client authentication is enabled, only clients that have keys stored in the Certificate Trust List file are can get WACS services. Other clients are rejected. You can only enable client authentication if you check *Enable HTTPS*.	**FALSE**
Certificate Trust List File Location	The full path to the certificate trust list file. You can only specify a value if you check *Enable HTTPS* and *Enable Client Authentication*.	Blank
Certificate Trust List Private Key Access Password	The password that protects access to the private keys in the Certificate Trust List file. You can only specify a value if you check *Enable HTTPS* and *Enable Client Authentication*.	Blank
Maximum HTTP Header Size	The maximum allowed size, in bytes, of the request and response HTTP header.	32768

Table 186: Concurrency properties (per connector)

Property	Description	Default Value
Maximum Concurrent Requests	The number of concurrent HTTP or HTTPS requests that each connector (HTTP, HTTP through Proxy, or HTTPS) can process simultaneously.	**150** The range of allowed values is 1 to 1000.

Table 187: Active directory configuration properties

Property	Description	Default Value
Krb5.ini File Location	The full path to a `krb5.ini` file that stores Kerberos configuration properties.	Blank
bscLogin.conf File Location	The full path to a `bscLogin.conf` file.	Blank

30.1.3 Connectivity Services Properties

The Connectivity service category includes the following services:

- Native Connectivity Service (hosted in standalone server)
- Native Connectivity Service (32-bit hosted in standalone server)
- Adaptive Connectivity Service (hosted in APS)

All services share the same configuration settings.

Table 188: Excel Data Access Service Properties

Property	Description	Default Value
Excel Data Access Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	The default value is 1200 seconds.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Excel Data Access Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the *Excel Data Access Cleanup Timeout (in seconds)* property.	The default value is 600 seconds.

Table 189: Service Operation Properties

Property	Description	Default Value
Remember You do not need to restart the server after changing the following Service Operation Properties.		
Connection Pooling	Either enables or disables the connection pool. Possible values are: • Enabled - With Timeout • Enabled - Without Timeout • Disabled **Note** The connection pool is a caching functionality that maintains connections in a reusable state for improving server performance.	Enabled - With Timeout
Connection Pool Timeout	Specifies the maximum idle time for connections in the pool (in minutes). **Note** This property is equivalent to the `Max Pool Time` parameter of the `cs.cfg` file. Disabling the pool is equivalent to `Max Pool Time` set to `0`. Enabling the pool without timeout is equivalent to `Max Pool Time` set to `-1`. Refer to *Data Access Guide* for more information.	60
Transient Object Inactivity Timeout	Specifies how many minutes to keep an unused temporary object in the server. The object is removed afterwards and its resources are reclaimed.	60
Transient Object Timer Interval	Specifies the time between activity checks (in minutes). At regular intervals, the server searches for candidate objects for removal.	5

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Enable HTTP Chunking	Either enables or disables the HTTP chunking. **Note** The HTTP chunking is relevant to 3-tier deployment only. It impacts the open/refresh document performance, because bigger responses mean less roundtrips when fetching large documents. Disabling the HTTP chunking is equivalent to *HTTP Chunk Size* set to **0**.	Enabled
HTTP Chunk Size	Specifies the size of the HTTP responses emitted by the server (in kilobytes).	**64**

Table 190: Low Level Tracing Properties

Property	Description	Default Value
Remember You do not need to restart the server after changing the following Low Level Tracing Properties.		
Enable Job Tracing	Enables the tracing of Connection Server jobs. **Note** It requires *Log Level* property to be set to *High*.	Disabled
Enable Middleware Tracing	Enables the tracing of all middleware. To trace specific middleware, you must configure the `cs.cfg` file and restart the server. **Note** It requires *Log Level* property to be set to *High*.	Disabled

Table 191: Active Data Sources Properties

Property	Description	Default Value
Caution You must restart the server after changing the following Active Data Sources Properties.		

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Activate Data Source	Allows you to select the data sources for which you want connections. This property works as a filter for drivers. You specify the active data sources to load the drivers you want to use. **Caution** The default server behavior is to load all available drivers. Use this setting to specialize servers. It is particularly useful when you deploy multiple CORBA servers on your network. **Remember** Only drivers for selected data sources are loaded. All the others are ignored. If you do not select any data sources, the server loads all available drivers. **Note** Verify in the server metrics that the selected data sources have been activated. The network layers and databases are displayed under *Connection Service Metrics*.	Unchecked
Network Layer	Specifies the network layer used by the connection. **Note** Only the non-localized name is considered. You can find the list of available network layers in the `driver.cfg` file, which is located in the **<connectionserver-install-dir>**`\connectionServer` directory.	• `ODBC` for native CORBA servers • `JDBC` for Adaptive CORBA server
Database	Specifies the database used by the connection. **Note** Only the non-localized name is considered. Database names can be regular expressions if they are pure ASCII strings. Patterns use GNU regexp syntax. Use the `.*` pattern to match any character. For example, the `MS SQL Server.*$` expression means all MS SQL Server databases are used. For more information about regular expressions, refer to the PERL website at http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions .	The field is empty until you enter a database name.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 192: Custom Data Access Service Properties

Property	Description	Default Value
Custom Data Access Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	The default value is 1200 seconds.
Custom Data Access Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the *Custom Data Access Cleanup Timeout (in seconds)* property.	The default value is 600 seconds.

Table 193: Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Table 194: Promotion Management Service Properties

Property	Description	Default Value
No configuration properties		

Table 195: Promotion Management ClearCase Service Properties

Property	Description	Default Value
No configuration properties		

Table 196: Visual Difference Service Properties

Property	Description	Default Value
No configuration properties		

Related Information

Common Server Properties [page 867]

30.1.4 Crystal Reports Services Properties

The Crystal Reports service category includes the following servers:

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Crystal Reports 2013 Report Application Server Properties
- Crystal Reports 2013 Processing Server

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Crystal Reports Cache Server Properties

Any properties that apply to both Crystal Reports Cache Servers and Crystal Reports Processing Servers should be set to the same value. For example, if you set the *Viewer Refresh Always Yields Current Data* setting to **TRUE** on the Cache Server, you should set the same property to **TRUE** on the Processing Server.

> **Note**
>
> When you modify any of these server properties, you must restart the server for the changes to take effect.

Table 197: Crystal Reports Cache Service Properties

Property	Description	Default Value
Viewer Refresh Always Yields Current Data	Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings. To specify a value on the report object, select the report in the CMC, and click *Default Settings* > *Viewing Server Group*.	The default value is **FALSE**.
Share Report Data Between Clients	Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is **TRUE**.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Crystal Reports Cache Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 20 minutes.
Security Cache Timeout (minutes)	Specifies the amount of time, in minutes, that the server uses cached logon credentials, report parameters, and database connection information to serve requests before querying the CMS.	The default value is 20 minutes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand reports. If the server receives a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (perhaps because important data changes very frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is 0 seconds.
Maximum Cache Size (KB)	Specifies the amount of hard disk space (in KB) that is used to cache reports. A large cache size may be necessary if the server needs to handle large numbers of reports, or reports that are especially complex.	The default value is 256000 KB.
Cache Files Directory	Specifies the location of the cache file directory.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Java VM Arguments	Specifies the command-line arguments that can be supplied to the JVM.	The default value is empty.
DLL Name	Specifies the name of the document-type plug-in that is currently loaded. This property is read-only.	rasprocReport

Crystal Reports Processing Server Properties

Any properties that apply to both Crystal Reports Cache Servers and Crystal Reports Processing Servers should be set to the same value. For example, if you set the *Viewer Refresh Always Yields Current Data* setting to **`TRUE`** on the Cache Server, you should set the same property to **`TRUE`** on the Processing Server.

Note

When you modify any of these server properties, you must restart the server for the changes to take effect.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 198: Crystal Reports Processing Service Properties

Property	Description	Default Value
Idle Job Timeout (minutes)	Specifies the length of time, in minutes, that the Crystal Reports Processing Server waits between requests for a given job.	The default value is 20 minutes.
Maximum Lifetime Jobs Per Child	Specifies the maximum number of jobs that each child process can manage per lifetime.	The default value is 1000.
Viewer Refresh Always Yields Current Data	Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings. To specify a value on the report object, select the report in the CMC, and click *Default Settings* > *Viewing Server Group*.	The default value is **FALSE**.
Share Report Data Between Clients	Specifies whether report data is shared between different clients. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is **TRUE**.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Crystal Reports Processing Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 20 minutes.
Maximum Concurrent Jobs (0 for automatic)	Specifies the maximum number of independent jobs allowed to run concurrently on the Crystal Reports Processing Server. If the value of this property is set to "0", the server applies a suitable value, based on the CPU and memory of the machine that the server is running on.	The default value is 0.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand reports. If the server receives a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (perhaps because important data changes very frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is 0.
Maximum Number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessary wasted by idle child processes.	The default value is 1 child.
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java Class Path	The name and path of the Java classes that are required by the server.	%CommonJavaLibDir%/procCR.jar
Java Child VM Arguments	Specifies the command-line arguments that are supplied to child processes that are created by the server.	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

Table 199: Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Crystal Reports 2013 Report Application Server Properties

> **Note**
>
> When you modify any of these properties, you must restart the server for the changes to take effect.

Table 200: Crystal Reports 2013 Viewing and Modification Service Properties

Property	Description	Default Value
Allow Report Jobs to Stay Connected to the Database until the Report Job is Closed	Specifies whether the report job will remain connected to the database until the process has been executed.	The default value is **FALSE**.
Browse Data Size (records)	Specifies the number of distinct records returned from the database when browsing through a particular field's values. The data is retrieved first from the client's cache - if it is available - and then from the server's cache. If the data is not in either cache, it is retrieved from the database.	The default value is 100 records.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Report Application Server (RAS) waits for requests from an idle client before timing out. Setting a value too low can cause a user's request to be closed prematurely, and setting a value that is too high can affect the server's scalability (for instance, if the `ReportClientDocument` object is not closed explicitly, the server will be waiting unnecessarily for an idle job to close).	The default value is 30 minutes.
Batch Size (records)	Specifies how many rows from the result set are returned by the database during each data transfer. For example, if 500 records are requested, and the Batch Size property is set to 100 records, the data will be returned in 5 separate batches of 100 rows. To improve the performance of your RAS, you must understand your network environment, database, and the type of requests in order to set the appropriate batch size.	The default value is 100 records.
Number of database records to read when previewing or refreshing a report (-1 for unlimited)	Specifies the number of database records that will be read when viewing or refreshing a report. This setting limits the number of records that the server retrieves from the database when a user runs a query or report. This setting is useful when you want to prevent users from running on-demand reports that return excessively large record sets. You may prefer to schedule such reports, both to make the reports available more quickly to users and to reduce the load on your database from these large queries.	The default value is 20000 records.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Maximum Concurrent Report Jobs (0 for unlimited)	Specifies the maximum number of independent jobs allowed to run concurrently on the RAS.	The default value is 75 jobs.
Oldest on-demand data given to a client (minutes)	Specifies the amount of time, in minutes, an on-demand report will serve cached report data.	The default value is 20 minutes.
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

Table 201: Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

Crystal Reports 2013 Processing Server Properties

Note

When you modify any of these properties, you must restart the server for the changes to take effect.

Table 202: Crystal Reports 2013 Processing Service Properties

Property	Description	Default Value
Idle Job Timeout (minutes)	Specifies the length of time, in minutes, that the Crystal Reports Processing Server waits between requests for a given job.	The default value is 20 minutes.
Maximum Lifetime Jobs Per Child	Specifies the maximum number of jobs that each child process can manage per lifetime.	The default value is 1000.
Viewer Refresh Always Yields Current Data	Specifies whether, when users explicitly refresh a report, all cached pages are ignored and new data is retrieved directly from the database. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings. To specify a value on the report object, select the report in the CMC, and click *Default Settings* > *Viewing Server Group*.	The default value is **`FALSE`**.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Share Report Data Between Clients	Specifies whether report data is shared between different clients. Specifies whether report data is shared between different clients. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is **TRUE**.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Crystal Reports Processing Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 20 minutes.
Maximum Concurrent Jobs (0 for automatic)	Specifies the maximum number of independent jobs allowed to run concurrently on the Crystal Reports Processing Server. If the value of this property is set to "0", the server applies a suitable value, based on the CPU and memory of the machine that the server is running on.	The default value is 0.
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand reports. If the server receives a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (perhaps because important data changes very frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set on a report object itself, and can vary from report to report; values specified on the report object override the server settings.	The default value is 0.
Maximum Number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessary wasted by idle child processes.	The default value is 1 child.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Temporary Directory	Specifies the directory where temporary files are created when necessary. **Note** You may encounter performance issues if this directory does not have adequate disk space.	%DefaultDataDir%/CrystalReports2013ProcessingServer/temp
Allow Report Jobs to Stay Connected to the Database until the Report Job is Closed	Specifies whether the report job will remain connected to the database until the job is closed.	The default value is FALSE.
Database Records Read When Previewing or Refreshing (0 for unlimited)	Specifies the number of database records that will be read when viewing or refreshing a report. This setting limits the number of records that the server retrieves from the database when a user runs a query or report. This setting is useful when you want to prevent users from running on-demand reports that return excessively large record sets. You may prefer to schedule such reports, both to make the reports available more quickly to users and to reduce the load on your database from these large queries.	The default value is 20000.

Table 203: Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

30.1.5 Analysis Services Properties

The Analysis services category includes the Adaptive Processing Server:

Table 204: Multi-Dimensional Analysis Service Properties

Property	Description	Default Value
Maximum Client Sessions	Specifies the maximum number of MDAS sessions that can simultaneously be open on the server. When the number of open sessions reaches this number, any additional attempts to start MDAS sessions result in a "server unavailable" error message. You can change this value to optimize MDAS performance, depending on your needs and available hardware, but increasing the value may result in performance issues for both the MDAS and the database. The default value of 15 sessions is a conservative estimate. For installations where user queries are small, you can increase this value significantly, whereas installations where user queries are large would require a lower value.	The default value is set to 15. The valid range is 1 to 100.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Maximum number of cells returned by a query	Specifies the number of cells that are returned to a user in a single query. The user is prevented from executing a query that returns an extremely large number of cells, consuming a large amount of memory. If the user's query exceeds this cell limit, the user receives an error message.	The default value is 100000 cells.
Maximum number of members returned when filtering	Specifies the number of members retrieved when filtering by member. A very large number of retrieved members can consume a large amount of memory.	The default value is 100000 members.

Table 205: BEx Web Applications Service Properties

Property	Description	Default Value
Maximum Client Sessions	The maximum number of client sessions allowed on the service.	The default value is 15 sessions.
SAP BW Master System	The name of the OLAP connection to the BW system that you created in the BI platform.	The default value is SAP_BW.
JCo Server RFC Destination	The name of the JCo Server RFS Destination that you entered in the BW system.	By default, this value is empty.
JCo Server Gateway Host	The name of the JCo Server Gateway Host that you defined in the BW system.	By default, this value is empty.
JCo Server Gateway Service	The name of the JCo Server Gateway Service that you defined in the BW system.	By default, this value is empty.
JCo Server Connection Count	Specifies the number of automatically created programs that can be used to handle calls from ABAP to Java for the service.	The default value is 3 connections.

30.1.6 Data Federation Services Properties

The Data Federation services category includes the Adaptive Processing Server:

Table 206: Data Federation Service Properties

Property	Description	Default Value
Max Connections	Specifies the maximum number of connections allowed on the server.	The default value is 32767.
Execution Pool Size	Specifies the maximum number of queries that can be executed in parallel at a given moment.	The default value is 10.
Connection Inactivity Timeout	Specifies the amount of time in seconds after which an inactive connection is closed.	The default value is 10800 seconds.
Statement Inactivity Timeout	Specifies the amount of time in seconds after which an inactive query statement is closed.	The default value is 600 seconds.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

30.1.7 Web Intelligence Services properties

The Web Intelligence services category includes the following servers:

- Adaptive Processing Server
- Web Intelligence Processing Server

Adaptive Processing Server settings

Table 207: Command Line Parameters

Property	Description	Default Value
Expand to Level	Specifies the level to which data is retrieved from BEx queries. By default, hierarchies are not expanded to a given level. Level00 is always the default level. You can change this behavior by adding this parameter to the command line, but if the value is set too high, Web Intelligence retrieves all of the hierarchy data, which can affect the performance and stability of the system.	`-Dsap.sl.bics.expandToLevel=n` n can be any integer between 0 and 99. If n=0, or if this parameter is not specified, hierarchies will not use the Expand to Level parameter.
Selection Option variable selection	Specifies the selection option for variable selection. If this property is set to interval, then the text box is not available and users can only enter start and end values in the Prompts dialog box. If this property is set to multivalue, then the "Type a value" text box is available and users can enter values for BW Selection Option variables. **Note** This property does not update local installations of Web Intelligence Rich Client. See the "Web Intelligence Rich Client Installation Guide" for information on updating the local registry for such installations.	`-Dsap.sl.bics.variableComplexSelectionMapping=n` where n can be either interval or multivalue. **Note** Prior to BI 4.1 SP05, the default value for this option was interval. If you add this property to the Adaptive Processing Server settings and set it to multivalue, then the following actions need to be done on existing documents: • A document needs to be purged. • The default values for query prompts need to be changed so that it is compatible with multivalue selection.

Table 208: Web Intelligence Monitoring Service properties

Property	Description	Default Value
Enable Monitoring	Specifies whether monitoring is enabled for the service.	`TRUE`
Monitoring Thread Loop Delay (seconds)	Specifies the amount of time, in seconds, between attempts that the service makes to ping clients.	300

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Default Monitored Resource Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	1200
Default Monitored Resource Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the Default Monitored Resource Cleanup Timeout property.	600
Enable Service Profiling		`TRUE`
Enable Service Activity Monitoring		`TRUE`

Table 209: Visualization Service properties

Property	Description	Default Value
Visualization Engine Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	1200
Visualization Engine Swap Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before swapping the client's session onto the hard disk. It is recommended that you specify a value that is lower than the value for the *Visualization Engine Cleanup Timeout (in seconds)* property.	600

Table 210: Rebean Service properties

Property	Description	Default value
No configuration properties		

Table 211: Document Recovery Service properties

Property	Description	Default value
No configuration properties		

Table 212: DSL Bridge Service properties

Property	Description	Default value
DSLBridge Engine Cleanup Timeout (in seconds)	Specifies the amount of time, in seconds, that the service waits for an inactive client before performing a cleanup of the client's session.	1200

Web Intelligence Processing Server properties

The Web Intelligence Processing Server properties are grouped into the following services:

- Information Engine
- Web Intelligence Core
- Web Intelligence Processing
- Web Intelligence Common

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Threshold settings are described in separate tables.

Table 213: Information Engine Service properties

Property	Description	Default Value
Enable List of Values Cache	Specifies whether caching is enabled for List of Values on the Web Intelligence Processing Server.	**TRUE**
List of Values Batch Size (entries)	Specifies the maximum number of entries (or values) for each List of Values batch.	1000
Maximum Custom Sort Size (entries)	Specifies the maximum number of entries in the custom sort.	100
Universe Cache Maximum Size (Universes)	Specifies the number of universes to be cached on the Web Intelligence Processing Server.	20
Maximum List of Values Size (entries)	Specifies the maximum number of entries (or values) for each List of Values.	50000

Table 214: Web Intelligence Core Service properties

Property	Description	Default Value
Timeout Before Recycling (seconds)	Specifies the time, in seconds, the server is idle before the Server Intelligence Agent (SIA) stops and restarts the server when the total number of documents processed is above the value specified with the *Maximum Documents Before Recycling* property.	1200
Idle Document Timeout (seconds)	Specifies the amount of time, in seconds, before the Web Intelligence Processing Server session will be swapped. Therefore, when the client is not generating requests during this period of time, the session will be swapped onto the hard disk, freeing up resources for an active session.	300 The valid range is 100 to 10000 seconds.
Server Polling Interval (seconds)	Specifies the interval, in seconds, that must pass before the server polls for new thread requests. When the server is in the polling phase, it performs cleanup actions like swapping unused documents to keep the server memory under the upper memory threshold.	120
Maximum Documents per User	Specifies the maximum number of active sessions (Web Intelligence documents) that can be associated with a user at any given time. Therefore, if 5, then the user can use up to 5 active sessions at once.	5 The valid range is 1 to 20.
Maximum Documents Before Recycling	Specifies the number of Web Intelligence documents that can be processed before the server will be considered for recycling. If the number of processed documents has been reached, and the server is idle, then the server is closed and the Server Intelligence Agent (SIA) starts a new instance of the server. However, there will be a time delay before a new instance of the server is started. The time delay is defined by the *Timeout Before Recycling* property.	50
Allow Document Map Maximum Size Errors	Specifies whether the **<Maximum Connections>** property is restricted. If this property is enabled, then the value set for the **<Maximum Connections>** property is recognized by the server; otherwise the property is disregarded.	**TRUE**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the server waits for a request from an idle connection. Setting a value that is too low can cause a request to close prematurely. Setting a value that is too high can caused requests to be queued while the server waits for idle requests to be closed.	20
Maximum Connections	Specifies the maximum number of simultaneous sessions that can be opened at one time. This is an approximate number; this setting does not count the inactive sessions that are swapped, or the session that is created to analyze the number of sessions. If this limit is reached and no other server is available to handle the request, the user will receive an error message. **Note** The **<Allow Document Map Maximum Size Errors>** property must be enabled for this property to be recognized by the server.	50 The valid range is 5 to 65535.
Enable Memory Analysis	Specifies whether memory analysis is enabled. If this property is enabled then the following properties will be active and recognized by the server: • **<Memory Maximum Threshold>** • **<Memory Upper Threshold>** • **<Memory Lower Threshold>** When the server's process memory is above the **<Memory Upper Threshold>**, the only operation that is allowed is saving documents. When the process memory is above the **<Memory Maximum Threshold>**, all operations stop and fail.	**TRUE**
Memory Lower Threshold (MB)	Specifies the lower threshold for memory consumption.	**3500**
Memory Upper Threshold (MB)	Specifies the upper threshold for memory consumption. The Web Intelligence Processing server restarts automatically when the Web Intelligence server memory reaches the upper threshold value.	**4500**
Memory Maximum Threshold (MB)	Specifies the maximum threshold for memory consumption.	**6000**
Enable APS Service Monitoring	Enables monitoring of the server by the APS service, hosted on the Adaptive processing server.	**TRUE**
Retry Count on APS Service ping failure	Specifies the number of times the server will try to reach the APS Service before deciding that it is unable to reach it.	3
APS Service Monitoring Thread Period	Specifies the period of delay between attempts to reach the APS Service.	300

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Enable Current Activity Logs	Specifies whether complete traces are generated in the server's log files. **Note** This property should be enabled only for debugging purposes when troubleshooting issues. Set to **FALSE** during normal operations.	**FALSE**

Table 215: Web Intelligence Processing Service properties

Property	Description	Default Value
Enable use of HTTP URL	Specifies whether the server is able to access files that are stored remotely.	**TRUE**
Proxy value	Specifies the address of your network's proxy server. It is only necessary to specify a value if your network has a proxy server and you attempting to access files that are stored remotely.	Blank

Table 216: Web Intelligence Common Service properties

Property	Description	Default Value
Cache Timeout (minutes)	Specifies the amount of time, in minutes, before the contents of the document cache will be cleared. The timeout depends on the most recent access date per document.	4370
Document Cache Clean-up Interval (minutes)	Specifies the time interval, in minutes, that the document cache is scanned and is checked against the **<Maximum Document Cache Size>**, **<Maximum Document Cache Reduction Space>**, and **<Maximum Document in Cache>** settings.	120
Disable Cache Sharing	Specifies whether cache sharing is disabled. By default cache sharing is enabled; which means that all Web Intelligence Processing Server instances will share the same cache. However, if you prefer to have one cache per instance of Web Intelligence Processing Server then you should enable this property.	**FALSE**
Enable Document Cache	Specifies whether the document cache is enabled. If the property is enabled, then the cache can be pre-loaded with scheduled Web Intelligence documents.	**TRUE**
Enable Real-Time Cache	Specifies whether the real-time cache is enabled. If the property is enabled, then the cache can be loaded dynamically. Therefore, the Web Intelligence Processing Server caches Web Intelligence documents when they are viewed. The server also caches the documents when they run as a scheduled job, if the pre-cache was enabled in the document.	**TRUE**
Maximum Document Cache Size (KB)	Specifies the maximum size of the document cache. Once this limit is reached the document cache will be cleared based on the **<Maximum Document Cache Reduction Space>** property.	1000000
Maximum Document Cache Reduction Space (percent)	Specifies the percentage of cache that is emptied to allow newer actions and results to be stored in the cache. Documents with the oldest "last access time" are purged.	70

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Maximum Character Stream Size (MB)	Specifies the maximum character stream size sent to the Web Intelligence client. **Note** If the *Maximum Character Stream Size* property is exceeded, then the Web Intelligence document will not be created and the client will receive an error message.	5 The valid range is 1 to 65535 MB.
Binary Stream Maximum Size (MB)	Specifies the maximum size, in MB, of a binary stream sent to the Web Intelligence client. **Note** If the *Binary Stream Maximum Size* property is exceeded, then the Web Intelligence document will not be created and the client will receive an error message.	50 The valid range is 1 to 65535 MB.
Images Directory	Specifies the location of the images directory.	Blank
Output Cache Directory	Specifies the location of the cache.	Blank

Table 217: General properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	86400

Related Information

Web Intelligence Server Memory Threshold Settings [page 898]

30.1.7.1 Web Intelligence Server Memory Threshold Settings

The following sections describe what happens on a Web Intelligence server when the Memory Maximum Threshold, Memory Upper Threshold, or Memory Lower Thresholds are reached.

Memory Lower Threshold

If the **<Memory Lower Threshold>** limit is reached, the server swaps out inactive documents onto the hard disk allocating additional memory for the documents which are active. Each user is allowed to have up to one active document instead of **<Maximum Documents per User>**.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Memory Upper Threshold

If this **<Memory Upper Threshold>** is reached, the following server actions will take place in order to free resources and protect the server:

- The server will reject new connections and new client calls. Only the option to *Save* Web Intelligence documents will be allowed. Users that request an action will receive a `Server Busy` message, and they will be notified that they should save any pending changes.
- The server will turn on system cleanup to free enough resources so that the amount of allocated memory is below the limit set by the **<Memory Upper Threshold>** property.
- The server tries to close read-only documents.
- If not enough memory was freed during system cleanup then the server will begin to close documents that are in *Editing* mode. The server will begin to close documents based on the LIFO protocol; the most recent active document will be purged from memory first. The server will continue to close documents until a safe level is reached; this level is based on the following calculation: **<Memory Upper Threshold>** - (20%*(**<Memory Upper Threshold>**)). For example, if the Memory Upper Threshold property is set to 4500MB then the safe level would be:

  ```
  4500MB - .20*4500MB = 3600MB
  ```

  The server cannot close documents when a client call is running. Any document that is refreshed or exported to another format or any other time consuming operation will not be closed when the server reaches this threshold. If the server cannot recover enough memory and is still above the **<Memory Upper Threshold>**, it restarts.

Memory Maximum Threshold

If the <Memory Maximum Threshold> limit is reached, all current operations abort. All client calls will be terminated. Once the a call terminates, the corresponding document will be closed.

30.1.8 Dashboards Services Properties

Dashboards Cache Server Properties

Table 218: Dashboards Cache Service Properties

Property	Description	Default Value
Maximum Cache Size (KB)	Specifies the amount of hard disk space (in KB) that is used to cache queries. A large cache size may be necessary if the server needs to handle large numbers of queries, or highly complex queries.	The default value is 256000 KB.
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the Dashboards Cache Server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 15 minutes.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Share Data Between Clients	Specifies whether report data is shared between different clients.	The default value is *TRUE*.
Oldest On-Demand Data Given to Clients (seconds)	Specifies the amount of time, in seconds, that the server uses cached data to meet requests from on-demand queries. If the server receive a request that can be met using data that was generated to meet a previous request, and the time elapsed since that data was generated is less than the value set here, then the server will reuse this data to meet the subsequent request. Reusing data in this way significantly improves system performance when multiple users need the same information. When setting this value, consider how important it is that your users receive up-to-date data. If it is very important that all users receive fresh data (important changes happen frequently) you may need to disallow this kind of data reuse by setting the value to 0. **Note** This property can be set in a report object itself; values specified on the report object override the server settings.	The default value is 0 seconds.
Security Cache Timeout (minutes)	Specifies the amount of time, in minutes, that the server uses cached logon credentials, query properties, and database connection information to serve requests before querying the CMS	The default value is 20 minutes.
Java VM Arguments	Specifies the command-line arguments that can be supplied to the JVM.	Xmx858M

Dashboards Processing Server Properties

Table 219: Dashboards Processing Service Properties

Property	Description	Default Value
Maximum Concurrent Jobs	Specifies the maximum number of independent jobs allowed to run concurrently on the server. If the value of this property is set to "0", the server applies a suitable value, based on the CPU and memory of the machine that the server is running on.	The default value is 0.
Maximum Lifetime Jobs Per Child	Specifies the maximum number of jobs that each child process can manage per lifetime.	The default value is 10000.
Maximum number of Prestarted Children	Specifies the maximum number of prestarted child processes that are allowed by the server. If this value is too low, the server creates child processes as soon as requests are made, and a user may experience latency. If this value is too high, system resources may be unnecessarily wasted by idle child processes.	The default value is 1.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Property	Description	Default Value
Idle Connection Timeout (minutes)	Specifies the amount of time, in minutes, that the server waits for a request from an idle connection. There is generally no need to modify the default value.	The default value is 15 minutes.
Idle Job Timeout (minutes)	Specifies the length of time (in minutes) that the server waits between requests for a given job.	The default value is 15 minutes.
Java Child VM Arguments	Specifies the command-line arguments that are supplied to child processes that are created by the server.	Xmx858M,Dswfinjection.lang.directory=%CommonJavaLibDir%,Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%

Table 220: Single Sign-On Service Properties

Property	Description	Default Value
Single Sign-On Expiry (seconds)	Specifies the time, in seconds, that an SSO connection is valid before expiring.	The default value is 86400 seconds.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

31 Server Metrics Appendix

31.1 About the Server Metrics Appendix

In this appendix unless otherwise stated, the term server refers to an SAP BusinessObjects server, and not to the machine that the BI platform is installed or running on.

Server metrics are not available on servers that are not running.

In addition to the metrics described in this appendix, the Monitoring application can also monitor these server states:

Table 221:

Server State	Description
Health State	The Health State indicates the general health of a server. These are the possible values: • 0 = Red (Danger) • 1 = Amber (Caution) • 2 = Green (Healthy)
Server Enabled State	This state indicates whether a server is enabled or disabled. These are the possible values: • 0 = Disabled • 1 = Enabled
Server Running State	This state indicates the running state of a server. These are the possible values: • 0 = STOPPED • 1 = STARTING • 2 = INITIALIZING • 3 = RUNNING • 4 = STOPPING • 5 = FAILED • 6 = RUNNING_WITH_ERRORS • 7 = RUNNING_WITH_WARNINGS

Note

For information about SAP BusinessObjects Explorer server properties and metrics, see the *SAP BusinessObjects Explorer Administrator's Guide*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Related Information

Analyzing server metrics [page 352]

31.1.1 Common Server Metrics

The following metrics describe the machine that the specified server is running on.

Table 222: Machine-specific metrics

Metric	Description
Machine Name	The host name of the machine that the server is running on.
Operating System	The operating system of the machine that the server is running on.
CPU Type	The type of Central Processing Units of the machine that the server is running on. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
CPUs	The number of CPUs that are available to the server. On multi-core hardware, this metric may report the number of logical CPUs, and not the number of physical processors. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
RAM (MB)	The amount of memory in megabytes that is available on the machine that the server is running on. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
Local Time	The local time.
Disk Size (GB)	The size of the disk that the BI platform is installed on, in gigabytes. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).
Used Disk Space (GB)	The amount of used space on the disk, in gigabytes, that the BI platform is installed on. This includes disk space that is used by other programs on the machine, and not just space used by the BI platform. This metric is not available on Adaptive Processing Servers or Web Application Container Servers (WACS).

The following metrics describe the specified SAP BusinessObjects server.

Table 223: Server-specific metrics

Metric	Description
Name Server	The name and port number of the CMS server that this server publishes its address to.
Registered Name	The internal name of the server. This is not the name that appears on the *Servers* screen of the CMC.
Version	The version of the server.
Start Time	The time that the server was most recently started.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
PID	The unique Process ID number for the server. The operating system of the machine that the server is running on generates the PID. The PID can be used to identify the specific server.
Host Name	A comma-separated list of host names that are currently being used by the server.
Host IP Address	A comma-separated list of IP Addresses that the server listens for requests on.
Request Port	The port from which the server receives requests from other servers. If the server is listening to requests on more than one IP Address, the request port for the server will always be the same. If any other process uses this request port, the server will not start. Ensure that other processes do not use this port.
Busy Server Threads	The number of server threads that are currently servicing a request. If this number is the same as the maximum thread pool size of the server, it indicates that the system can't process additional requests in parallel and that new requests may have to wait for busy threads to become available.

Table 224: Auditing Metrics

Metric	Description
Current Number of Auditing Events in the Queue	The number of auditing events that an Auditee has recorded, but which have not yet been retrieved by the CMS Auditor. If this number increases without bound, it could indicate that Auditing is not configured correctly or that the system is heavily loaded and generating audit events faster than the Auditor can retrieve them. **Note** When stopping a server, first disable it and wait for this metric to reach “0”. Otherwise you may have auditing events that remain in the queue and do not reach the Auditing Data Store until the server is restarted and the CMS polls for them.

Table 225: Logging Service Metrics

Metric	Description
Logging Directory	Log files for the server are available in this location.

31.1.2 Central Management Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Central Management Servers (CMS).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 226: Central Management Server Metrics

Metric	Description
Connection to Auditing Database is Established	Indicates whether the CMS has a healthy connection to the auditing database. A value of “1” indicates that there is a connection. A value of “0” indicates that there is no connection to the auditing database. If the CMS is an auditor, this value should be “1”. If it is “0”, investigate why a connection to the auditing database cannot be established.
CMS Auditor	Indicates if the CMS Is acting as an auditor. A value of “1” indicates that the CMS is acting as an auditor. A value of “0” indicates that the CMS is not acting as an auditor.
Auditing Database Connection Name	The name of the auditing database connection. This is not necessarily the name of the auditing database itself. If this metric is empty, it indicates that a connection to the auditing database cannot be established.
Auditing Database User Name	The name of the user account used to connect to the auditing database.
Auditing Database Last Updated On	The most recent date and time that the CMS successfully started to retrieve events from an auditee. If the CMS is an auditor, this metric must show a time that is close to the time that the “Metrics” screen is loaded. If this value is more than two hours prior to the time that the screen is loaded, it may indicate that auditing is not working properly.
Auditing Thread Last Polling Cycle Duration (seconds)	The duration of the last polling cycle in seconds. This indicates the maximum delay for event data to reach the auditing database during the previous polling cycle. • A value of less than 20 minutes indicates a healthy system. • A value between 20 minutes and 2 hours indicates a busy system. • A value of greater than 2 hours indicates a very busy system. If this state persists and you consider the delay too long, it is recommended that you either update your deployment to all the auditing database to receive data at a higher rate or decrease the number of auditing events that your system tracks.
Auditing Thread Utilization	The percentage of the polling cycle the auditor CMS spends collecting data from auditees. The remainder is time spent resting between polls. If this value this reaches 100%, the auditor is still collecting data from the auditees when the next poll is due to begin. This may cause delays in the events reaching the auditing database. If the Thread Utilization frequently reaches 100%, and remains at this rate for several days, it is recommend you either update your deployment to allow the auditing database to receive data at a higher rate, or decrease the number of auditing events that your system tracks.
Clustered CMS Servers	A semicolon-separated list of the host names and port numbers of the running Central Management Servers in the cluster.
Number of Sessions Established by Concurrent Users	The total number of sessions for users with concurrent licensing.
Number of Sessions Established by Named Users	The total number of sessions for users with named licensing.
Peak Number of User Sessions Since Startup	The peak number of concurrent user sessions that the CMS has handled since it was started.
Number of Sessions Established by Servers	The number of concurrent sessions that BI platform servers have created with the CMS. If this number is greater than 250, create an additional CMS.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Number of Sessions Established by All Users	The number of concurrent user sessions that are being handled by the CMS when the *Metrics* screen loads. The larger this number is, the larger the number of users that are using the system is. If this number is greater than 250, create an additional CMS.
Failed Jobs	The number of failed jobs in the system.
Pending Jobs	The number of jobs that are scheduled, but not ready, to run because the scheduled time or event has not arrived.
Running Jobs	The number of currently running jobs.
Completed Jobs	The number of completed jobs in the system.
Waiting Jobs	The number of jobs in the system that are scheduled and waiting for free resources.
Concurrent User Licenses	The number of Concurrent User licenses as indicated by the key code.
Named User Licenses	The number of Named User licenses as indicated by the key code
Build Date	The build date of the CMS.
System Database Connection Name	The name of the CMS system database connection. This is not necessarily the name of the CMS system database itself.
System Database Server Name	The name of the server where the CMS system database is running. This is not necessarily the name of the CMS system database itself.
System Database User Name	The name of the user account used to connect to the CMS system database.
Data Source Name	The name of the CMS system database connection.
Build Number	The build number of the CMS. This number can be used to identify the version of SAP BusinessObjects Business Intelligence platform that you have installed.
Product Version	The product version of the CMS.
Resource Version	The resource version of the CMS.
Average Commit Response Time Since Startup (msec)	The average length of time in milliseconds that it took the CMS to perform commit operations since the server was started. A response time greater than 1000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Average Query Response Time Since Startup (msec)	The average length of time in milliseconds that it took the CMS to perform query operations since the server was started. A response time greater than 1000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Longest Commit Response Time Since Startup (msec)	The longest length of time in milliseconds that the it took the CMS to perform commit operations since the server was started. A response time greater than 10000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Longest Query Response Time Since Startup (msec)	The longest length of time in milliseconds that the it took the CMS to perform query operations since the server was started. A response time greater than 10000 milliseconds may indicate a need to tune the CMS or the CMS system database.
Number of Commits Since Startup	The number of commits to the CMS system database since the server was started.
Number of Queries Since Startup	The total number of database queries since the server was started. A large number may indicate a more active or heavily loaded system.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Number of User Logons Since Startup	The number of user logons since the server was started. A large number may indicate a more active or heavily loaded system.
Established System Database Connections	The number of connections to the CMS system database that the CMS was able to establish. If a database connection is lost, the CMS attempts to restore the connection. If the number of established database connections is consistently lower than the number of system database connections specified by the *System Database Connections Requested* property (*Central Management Service* area of the *Properties* screen), it may indicate that the CMS can't acquire additional connections, and that the system is not functioning optimally. A potential solution is to configure the database server to allow more database connections for the CMS.
Currently Used System Database Connections	The number of connections to the CMS system database that the CMS is currently using. The number of connections that are being currently used may be smaller than or equal to the number of established system database connections. If the number of established connections and the number of used connections are identical for some time, this may indicate a bottleneck. Increasing the value for the *System Database Connections Requested* property on the *Properties* screen may improve the performance of the CMS. Tuning the CMS system database may also improve performance.
Pending System Database Requests	The number of requests for the CMS system database that are waiting for an available connection. If this number is high, consider increasing the value for the *System Database Connections Requested* property. Tuning the CMS system database may also improve performance.
Number of Objects in CMS System Cache	The total number of objects that are currently in the CMS system cache.
Number of Objects in CMS System DB	The total number of objects that are currently in the CMS system database.
Existing Concurrent User Accounts	The total number of existing users with concurrent licensing in the cluster.
Existing Named User Accounts	The total number of existing users with named licensing in the cluster.

31.1.3 Connection Server Metrics

The following metrics are specific to the Connection Server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 227: Connectivity Service metrics

Metric	Description
Data Sources	Lists in a table the data sources activated via the *Properties* page. Displays the following information for each network layer and database pair: • *Status* (*Loaded* or *Failed!*): current status of the driver • *Available Connections: number of pool connections that can be used* • *Jobs (CORBA): number of jobs that are being processed (2-tier deployment)* • *Jobs (HTTP): number of jobs that are being processed processing (web tier deployment)* **Note** For more information about connection pools, refer to the *Data Access Guide*.

31.1.4 Event Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Event Servers.

Table 228: Event Service Metrics

Metric	Description
List of Monitored Files	A table that lists the files that are being monitored by the Event Server. The "File-name" column displays the name and path of the file. The "Last Notified Time" column displays the latest timestamp of when the server did a poll and found that the file exists.
Monitored Files	The total number of files that are being monitored by the Event Server.

31.1.5 File Repository Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Input and Output File Repository Servers.

Table 229: Filestore Service Metrics

Metric	Description
Active Files	The number of files in the File Repository Server that are currently being accessed.
Data Written (MB)	The total number of megabytes written to files on the server.
Data Sent (MB)	The total number of megabytes read from files on the server.
List of Active Files	A table that displays the files in the File Repository Server that are currently being accessed.
Active Connections	The total number of active connections from clients and to other servers.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Available Disk Space in Root Directory (GB)	The total amount of available space on the disk containing the server's executable file, in gigabytes.
Free Disk Space in Root Directory (GB)	The total amount of free space on the disk containing the server's executable file, in gigabytes.
Total Disk Space in Root Directory (GB)	The total disk space on the disk containing the server's executable file, in gigabytes.
Available Disk Space in Root Directory (%)	The amount of available disk space, in percentage, on the disk containing the server's executable file.

31.1.6 Adaptive Processing Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Adaptive Processing Servers.

Table 230: Adaptive Processing Server metrics

Metric	Description
Threads in Transport Layer	The total number of threads in all thread pools of the transport layer.
Transport Layer Thread Pool Size	The total number of shared transport layer threads. These threads can be used by any of the hosted services on the Adaptive Processing Server.
Available Processors	The number of processors that are available to the Java Virtual Machine (JVM) on which the server is running.
Maximum Memory (MB)	The maximum amount of memory, in megabytes, that the Java virtual machine will attempt to use.
Free Memory (MB)	The amount of memory, in megabytes, that is available to the JVM for allocating new objects.
Total Memory (MB)	The total amount of memory, in megabytes, in the Java virtual machine. This value may vary over time, depending on the host environment.
CPU Usage Percentage (last 5 minutes)	The percentage of total CPU time used by the server during the previous five minutes. For example, if a single thread fully utilizes one CPU of a four-CPU system, the utilization is 25%. All processors allocated to the JVM are considered. A value of greater than 80% may indicate a CPU bottleneck.
CPU Usage Percentage (last 15 minutes)	The percentage of total CPU time used by the server during the previous 15 minutes. For example, if a single thread fully utilizes one CPU of a four-CPU system, the utilization is 25%. All processors allocated to the JVM are considered. A value of greater than 70% may indicate a bottleneck.
Percentage of stopped system during GC (last 5 minutes)	Percentages of stopped system while Garbage Collections (GC) were running during the last five minutes. In this state all APS services are prevented from executing while the virtual machine performs a critical stage of garbage collection that requires exclusive access. Generally, a low single-digit value should be the normal behavior, even under load. A double-digit value over time might indicate an issue of low throughput and needs to be investigated.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Percentage of stopped system during GC (last 15 minutes)	Percentages of stopped system while Garbage Collections (GC) were running during the last 15 minutes. In this state all APS services are prevented from executing while the virtual machine performs a critical stage of garbage collection that requires exclusive access. Generally, a low single-digit value should be the normal behavior, even under load. A double-digit value over time might indicate an issue of low throughput and needs to be investigated.
Number of page faults during GC (last 5 minutes)	The number of page faults that have occurred while Garbage Collections were running during the previous five minutes. Any value greater than 0 indicates a system under heavy load and low memory conditions.
Number of page faults during GC (last 15 minutes)	The number of page faults that have occurred while Garbage Collections were running during the last 15 minutes. Any value greater than 0 indicates a system under heavy load and low memory conditions.
Number of Full GCs	The number of full Garbage Collections since the server has started. A rapid increase in this value may indicate a system under low memory conditions.
JVM Lock Contention Count	The number of synchronized objects that have threads that are waiting for access. Any value consistently greater than 0 may indicate threads that will not run again. Initiate a Thread Dump to obtain more information about the cause of the problem.
JVM Debug Info	Debugging information about the SAP Java Virtual Machine, including the state, port, and attached client, if available.
JVM Version Info	Version information about the SAP Java Virtual Machine.
JVM Deadlocked Threads Counter	The number of threads that are deadlocked. Any value greater than 0 indicates threads that will not run again. Initiate a Thread Dump to obtain more information about the cause of the problem.
JVM Trace Flags	The trace flags that are currently turned on for the JVM. This indicates the level of tracing of the JVM.
Services	A comma-separated list of the services that the server hosts.

Table 231: DSL Bridge Service metrics

Metric	Description
DSLServiceMetrics.queryCount	The number of data requests that are open between clients and the service
DSLServiceMetrics.activeConnectionCount	The number of connections that are currently open between clients and the service.
DSLServiceMetrics.activeSessionCount	The number of sessions that are currently open between clients and the service.
DSLServiceMetrics.activeOLAPConnection Count	The number of connections that are currently open between OLAP clients and the service.

Table 232: Client Auditing Proxy Service metrics

Metric	Description
Number of Audit Events Received Since Server Startup	The number of client auditing events that the service has received since it was started. This metric can be used to verify that client auditing has been configured correctly. Values greater than "0" indicate that auditing events from clients are being successfully routed through this Client Auditing Service.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 233: Platform Search Service metrics

Metric	Description
Number of Successful Extraction Attempts since the Service Start	The number of successful attempts for extracting documents since the Platform Search Service was started.
Last Index Update Timestamp	The date and time when the last index update happened.
Last Content Store Generation Timestamp	The date and time when the last content store was generated.
Number of failed extraction attempts since the service start	The number of failed attempts for extracting documents since the Platform Search Service was started.
Service Available	TRUE if the service is available. Otherwise FALSE.
Indexing Running	TRUE if the indexing is running. Otherwise FALSE.
Number of Documents Indexed	The displays the number of documents that were indexed since the service was started.

Table 234: Multi-Dimensional Analysis Service metrics

Metric	Description
Session Count	The current number of connections from MDAS clients to the server.
Cube Count	The number of data sources that are being used to supply data to the connections that have not timed out.
Query Count	The number of data requests that are open between MDAS clients and the server.

Table 235: Data Federation Service metrics

Metric	Description
Number of Running Queries	The total number of running queries (consuming memory or not).
Number of Connections	The total number of user connections to data federation query engine.
Total Bytes Transferred from Data Sources	The amount of data read from the data sources (in bytes).
Total Records Transferred from Data Sources	The total number of rows read from the data sources.
Total Bytes Produced by Query Execution	The amount of data produced as output of queries (in bytes).
Total Records Produced by Query Execution	The total number of rows produced as output of queries.
Number of Queries Consuming Memory	The total number of running queries consuming memory.
Total Bytes of Memory Used by Query Execution	The amount of memory currently used by the running queries (in bytes).
Total Bytes of Disk Used by Query Execution	The amount of disk currently used by the running queries (in bytes).
Number of Queries Using Disk	The total number of running queries using disk.
Number of Queries Waiting for Resources	The total number of running queries currently waiting for execution.
Number of Active Threads	The total number of active threads used for used for execution of requests.
Total Bytes of Memory Used by Metadata Cache	The amount of memory used for caching metadata, statistics and connectors configuration (in bytes).
Number of Failed Queries	The total number of failed queries (exception raised).
Number of Queries in Query Analyze Step	The total number of running queries currently in analyze step.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Number of Queries in Query Optimization Step	The total number of running queries currently in optimization step.
Number of Queries in Query Execution Step	The total number of running queries currently in execution step.
Number of Loaded Connectors	The total number of connectors loaded in the service.
Number of Active Connections to Loaded Connectors	The total number of active connections to connectors loaded in the service.
Data Federation Service is available	*TRUE* if the service is available. Otherwise, *FALSE*.

Table 236: Connectivity Service metrics

Metric	Description
Data Sources	Lists in a table the data sources activated on the *Properties* page. Displays the following information for each network layer and database pair: • Status ("Loaded" or "Failed"): The current status of the driver • Available connections: The number of pool connections that can be used • Jobs (CORBA): The number of jobs that are being processed (in a 2-tier deployment) • Jobs (HTTP: The number of jobs that are being processed (in a web-tier deployment) For more information about connection pools, see the *Data Access Guide*.

Table 237: Monitoring Service metrics

Metric	Description
Average Watch State Computation Time for Last 15 Cycles (msec)	The average time required for computing the watch state over the last 15 cycles, for this monitoring service instance.
Number of User Created Metrics	The total number of user-created metrics in the cluster, for all users.
Number of Watches	The total number of watches in the cluster, including both disabled and enabled watches.
serviceBean.monitoringAppPropEnabled	TRUE if the Monitoring application is enabled. Otherwise FALSE. This metric matches the setting on the Monitoring Application Properties page in the CMC.
Monitoring Metrics Refresh Interval (seconds)	The refresh interval currently being used by this monitoring service instance. At service start-up, this metric is initialized to the setting on the Monitoring Application Properties page in the CMC at that time, so at other times the metric may be different from the current setting on the CMC page.
Service Available	TRUE if this monitoring service is active. Otherwise FALSE. Only one monitoring service is active in the cluster.
Number of Trended Metrics	The total number of metrics currently being recorded into the monitoring database.

Table 238: BEx Web Applications Service metrics

Metric	Description
Session Count	A count of the total number of sessions active within a BEx Web Applications Service.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

31.1.7 Web Application Container Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Web Application Container Servers.

> **Note**
>
> Web Application Container Servers also have all of the metrics that are described under the Adaptive Processing Server Metrics section.

Table 239: Web Application Container Server Metrics

Metric	Description
List of Running WACS Connectors	A list of all running connectors on the server. If you do not see all of the connectors (HTTP, HTTPS and HTTP through proxy), it indicates either that the connector is not enabled or that it failed during startup
WACS Connector(s) Failed at Startup	Whether there are any failed connectors. If true, at least one connector failed to start. If false, all connectors are running. Do not run a server when one or more connectors has failed to start; you must troubleshoot the server to ensure that all connectors start properly.

Related Information

Adaptive Processing Server Metrics [page 909]

31.1.8 Adaptive Job Server Metrics

Table 240: Job Server Metrics

Metric	Description
Received Job Requests	The number of jobs that were supposed to have run on the server.
Concurrent Jobs	The number of jobs that are currently running on the server. If this number is high, the server is busy.
Peak Jobs	The maximum number of concurrent jobs that have run at the same time on the server. This number never goes down until the server is restarted.
Failed Job Creations	The number of jobs that failed on the server.
Temporary Directory	The directory where temporary files are created. This can be specified on the *Properties* screen for the server. You may encounter issues if this directory does not have adequate disk space.
File System Destination Default Settings Valid	*TRUE* if the server is able to send documents to the File System Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
FTP Destination Default Settings Valid	*TRUE* if the server is able to send documents to the FTP Server Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
Inbox Destination Default Settings Valid	*TRUE* if the server is able to send objects to the Inbox Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
Email Destination Default Settings Valid	*TRUE* if the server is able to send objects to the Email Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.
Scheduling Services	A table that displays the services that are running on the server.
Children	A table that displays the child processes that are running on the server.
SAP StreamWork Destination Default Settings valid	*TRUE* if the server is able to send objects to the SAP StreamWork Destination that is specified on the *Destination* screen for the server. Otherwise, *FALSE*.

The following table describes the metrics for each Scheduling Service that is running on the server.

Table 241: Scheduling Service Metrics

Metric	Description
Scheduling Service	The name of the service.
Received Job Requests	The number of jobs that were supposed to have run on the service.
Concurrent Jobs	The number of concurrent jobs that are currently running on the service. If this number is high, the service is busy.
Peak Jobs	The maximum number of concurrent jobs that have run at the same time on the service.
Maximum Concurrent Jobs Allowed	The number of concurrent independent processes (child processes) that the service allows. This can be specified on the *Properties* screen for the server.
Failed Job Creations	The number of jobs that failed on the service.

The following table describes the metrics for each child process that is running on the server.

Table 242: Child Metrics

Metric	Description
Scheduling Service	The name of the child process.
PID	The child process's identifier.
Received Job Requests	The number of jobs that were supposed to have run on the child process.
Concurrent Jobs	The number of concurrent jobs that are currently running on the child process. Normally this number must be “1”.
Peak Jobs	The maximum number of concurrent jobs that have run at the same time on the child process.
Maximum Jobs Allowed	The number of concurrent jobs that the child process allows.
Comm. Failures	The number of communication failures with the parent Adaptive Job Server that have occurred. If this number is large, the child process will restart.
Initializing	*TRUE* if the child process is in the process of initializing. Otherwise, *FALSE*.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Shutting Down	*TRUE* if the child process is in the process of shutting down. Otherwise, *FALSE*.

31.1.9 Crystal Reports Server Metrics

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports Processing and Crystal Reports 2013 Processing Servers.

Table 243: Crystal Reports Processing Server Metrics

Metric	Description
Open Jobs	A table listing of the jobs that are currently being run on the server. The table includes the ID and Name of the document, the name of the user running the job, the date that the document was last accessed, and the amount of time that the job has been running.
Number of Requests Served	The total number of requests that the server has served since it started.
Number of Open Jobs	The number of currently jobs that the server and its child processes are currently processing.
Object Type	The type of InfoObject that the server primarily deals with. The value for this metric does not change.
Average Processing Time (ms)	The average time, in milliseconds, the server has spent processing the last 500 requests that the server has received. If this number is consistently high and growing, consider creating additional servers on other machines.
Maximum Processing Time (ms)	The maximum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Minimum Processing Time (ms)	The minimum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Number of Queued Requests	The number of requests that are either waiting to be processed or are being processed. If this number is consistently high and growing, consider creating additional servers on other machines.
Object Dll Name	The name of the processing plug-in for the server. The value of this metric does not change.
Number of Open Connections	The number of connections that are currently open between the server and clients.
Request Failure Rate	The number of requests that the server failed to process as a percentage of the last 500 requests that the server has received.
Data Transferred (KB)	The total amount of data, in kilobytes, that have been transferred to clients since the server was started.
Number of Requests Failed	The number of requests that the server was unable to complete since the server started.
Maximum Number of Child Processes	The maximum number of concurrent child processes that are allowed on the server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports Cache Servers.

Table 244: Crystal Reports Cache Server Metrics

Metric	Description
Cache Hit Rate (%)	The percentage of requests, over the last 500 requests, that have been served with cached data.
Connected Processing Servers	A table listing of the Crystal Reports Processing servers in your deployment. The table lists the name of the server and the number of connections that are currently open with the server.
Number of Requests Served	The total number of requests that the server has served since it started.
Object Type	The type of InfoObject that the server primarily deals with. The value for this metric does not change.
Average Processing Time (msec)	The average time, in milliseconds, the server has spent processing the last 500 requests that the server has received. If this number is consistently high and growing, consider creating additional servers on other machines.
Maximum Processing Time (msec)	The maximum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Minimum Processing Time (msec)	The minimum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Number of Queued Requests	The number of requests that are either waiting to be processed or are being processed. If this number is consistently high and growing, consider creating additional servers on other machines.
Object Dll Name	The name of the processing plug-in for the server. The value of this metric does not change.
Cache Size	The amount of data, in kilobytes, that is currently being cached by the server on the disk.
Number of Open Connections	The number of connections that are currently open between the server and clients.
Data Transferred (KB)	The total amount of data, in kilobytes, that have been transferred to clients since the server was started.

The following table describes the server metrics that appear on the *Metrics* screen for Crystal Reports 2013 Report Application Servers.

Table 245: Crystal Reports 2013 Report Application Server Metrics

Metric	Description
metric_currentdoccount **Note** This metric appears as "document_s_" on the Monitoring page in the CMC.	The number of documents that are currently being processed by the server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
metric_totaldoccount **Note** This metric appears as "document_s_" on the Monitoring page in the CMC.	The number of documents that have been processed by the server since it started.
metric_currentagentthreadcount **Note** This metric appears as "agent thread_s_" on the Monitoring page in the CMC.	The number of threads that are currently being processed by the server.
metric_totalagentthreadcount **Note** This metric appears as "agent thread_s_" on the Monitoring page in the CMC.	The number of threads that have been processed by the server since it started.

31.1.10 Web Intelligence Server Metrics

Table 246: Web Intelligence Processing Service Metrics

Metric	Description
Cache size (Kb)	The current amount, in kilobytes, of data that is stored in the cache.
Number of out-of-date documents in cache	The number of documents deleted from the cache because there were too old, since the server was started.
Cache high mark count	The number of times that the cache has reached the maximum size allowed on the server since it was started.
CPU usage (%)	The percentage of total CPU time spent by the server since the server was started.
Total CPU time (seconds)	The total CPU time, in seconds, spent by the server since it was started.
Memory high threshold count	The number of times that the high memory threshold has been reached on the server since it was started.
Memory max threshold count	The number of times that the maximum memory threshold has been reached on the server since it was started.
Virtual memory size (Mb)	The total amount of memory, in megabytes, that are assigned to the server.
Current number of client calls	The current number of CORBA calls that the server is processing.
Number of remote extension errors	The number of times the server has failed to connect to a remote extension service hosted by an Adaptive Processing Server.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Current number of tasks	The current number of tasks that are being executed on the server.
Total number of client calls	The total number of CORBA calls that the server has received since it was started.
Total number of tasks	The total number of tasks that have been executed on the server since it was started.
Idle time (seconds)	The amount of time, in seconds, that have elapsed since the last request that the server has received from a client.
Current number of active sessions	The current number of sessions that are able to accept requests from clients.
Number of documents opened from cache	The number of documents for which the last request result has been directly read from the cache.
Number of documents	The number of documents that are currently open on the server.
Current number of sessions	The current number of sessions that have been created on the server.
Number of document swap	The number of documents for which a cleanup thread has scheduled swap requests.
Number of swapped documents	The number of documents that have been swapped by swap requests.
Number of sessions timeout	The number of sessions that have timed out since the server was started.
Total number of sessions	The number of sessions that have been created on the server since the server was started.
Number of users	The total number of users that are connected to the server.
Number of active threads	The number of threads serving requests received by the server (asynchronism threadpool).
Total number of threads	The total number of threads that have been created since the server was started (asynchronism threadpool).

31.1.11 Dashboards Server Metrics

Table 247: Dashboards Processing Server Metrics

Metric	Description
Open Jobs	A table listing of the jobs that are currently being run on the server. The table includes the ID and Name of the document, the name of the user running the job, the date that the document was last accessed, and the amount of time that the job has been running.
Number of Requests Served	The total number of requests that the server has served since it started.
Number of Open Jobs	The number of currently jobs that the server and its child processes are currently processing.
Object Type	The type of InfoObject that the server primarily deals with. The value for this metric does not change.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Average Processing Time (msec)	The average time, in milliseconds, the server has spent processing the last 500 requests that the server has received. If this number is consistently high and growing, consider creating additional servers on other machines.
Maximum Processing Time (msec)	The maximum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Minimum Processing Time (msec)	The minimum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Number of Queued Requests	The number of requests that are either waiting to be processed or are being processed. If this number is consistently high and growing, consider creating additional servers on other machines.
Object Dll Name	The name of the processing plug-in for the server. The value of this metric does not change.
Number of Open Connections	The number of connections that are currently open between the server and clients.
Request Failure Rate	The number of requests that the server failed to process as a percentage of the last 500 requests that the server has received.
Data Transferred (KB)	The total amount of data, in kilobytes, that have been transferred to clients since the server was started.
Number of Requests Failed	The number of requests that the server was unable to complete since the server started.
Maximum Number of Child Processes	The maximum number of concurrent child processes that are allowed on the server.

Table 248: Cache Server Metrics

Metric	Description
Cache Hit Rate (%)	The percentage of requests, over the last 500 requests, that have been served with cached data.
Connected Processing Servers	A table listing of the Dashboards Processing servers in your deployment. The table lists the name of the server and the number of connections that are currently open with the server.
Number of Requests Served	The total number of requests that the server has served since it started.
Object Type	The type of InfoObject that the server primarily deals with. The value for this metric does not change.
Average Processing Time (msec)	The average time, in milliseconds, the server has spent processing the last 500 requests that the server has received. If this number is consistently high and growing, consider creating additional servers on other machines.
Maximum Processing Time (msec)	The maximum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.
Minimum Processing Time (msec)	The minimum time, in milliseconds, that the server has spent processing one of the last 500 requests. If this number is consistently high and growing, consider creating additional servers on other machines.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Metric	Description
Number of Queued Requests	The number of requests that are either waiting to be processed or are being processed. If this number is consistently high and growing, consider creating additional servers on other machines.
Object Dll Name	The name of the processing plug-in for the server. The value of this metric does not change.
Cache Size (KB)	The amount of data, in kilobytes, that is currently being cached by the server on the disk.
Number of Open Connections	The number of connections to clients that are currently open.
Data Transferred (KB)	The total amount of data, in kilobytes, that have been transferred to clients since the server was started.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

32 Server and Node Placeholder Appendix

32.1 Server and node placeholders

With the exception of *%SERVER_FRIENDLY_NAME%* and *%SERVER_NAME%*, these placeholders apply to all of the servers on the same node.

Table 249: Placeholders

Placeholder	Description	Default values
%AuditingDatabaseConnection%	The Auditing Database connection used by the CMS.	This value is specified during installation.
%AuditingDatabaseDriver%	The type of database driver that is used to connect to the auditing database.	On Windows, the default value is sqlserverauditdbss.
%BINDIR%	The folder where SAP BusinessObjects Business Intelligence platform 64-bit binaries are located.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\win64_x64. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<platform>**/
%BINDIR32%	The folder where SAP BusinessObjects Business Intelligence platform 32-bit binaries are located.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\win32_x86. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<platform>**/
%CACHESERVER_EXE%	The name of the executable for the Crystal Reports Cache Server.	On Windows, crcache.exe. On UNIX, boe_crcached.bin.
%CMS_EXE%	The name of the executable for the Central Management Server.	On Windows, cms.exe. On UNIX, boe_cmsd.
%CONNECTIONSERVER32_EXE%	The name of the executable for the 32-bit Connection Server.	On Windows, ConnectionServer32.exe. On UNIX, ConnectionServer32.
%CONNECTIONSERVER_DIR%	The root folder of the Connection Server.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/dataAccess/connectionServer
%CONNECTIONSERVER_EXE%	The name of the executable for the 64-bit Connection Server.	On Windows, ConnectionServer.exe. On UNIX, ConnectionServer.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%CR2013_BINDIR%	The directory where Crystal Reports 2013 server binaries are located.	On Windows, **<INSTALLDIR>**\SAP BusinessObjectsEnterprise XI 4.0\win32_x86. On UNIX, the directory will be similar to: **<INSTALLDIR>**/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9.
%CR2013_DefaultWorkingDir%	The default working directory for Crystal Reports 2013 servers.	On Windows, **<INSTALLDIR>**\SAP BusinessObjectsEnterprise XI 4.0\win32_x86. On UNIX, the directory will be similar to: **<INSTALLDIR>**/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9.
%CRYSTALRAS_EXE%	The Name of the executable for the Report Application Server.	On Windows, crystalras.exe. On UNIX, boe_crystalrasd.
%CR_ODBCINI%	The name and path of the .odbc.ini file is located.	On UNIX, **<INSTALLDIR>**/bobje/odbc.ini. On Windows, this is an empty string.
%CommonJavaBundlesDir%	The folder where shared OSGI bundles are located.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/java/lib/bundles.
%CommonJavaLibDir%	The folder where the common Java libraries are located.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\java\lib. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/java/lib.
%DLLEXT%	The default extension of a .dll or .so file.	On Windows, .dll. On UNIX, .so.
%DLLPATH%	The name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories where the interpreter will search for executable files.	On Windows, "Path". On UNIX, "LD_LIBRARY_PATH".
%DLLPATH32%	On Solaris 32-bit systems, The name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories where the interpreter will search for executable files.	On Solaris machines, "LD_LIBRARY_PATH_32". This placeholder is an empty string on other operating systems.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%DLLPATH64%	On Solaris 64-bit systems, the name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories there the interpreter will search for executable files.	On Solaris machines, "LD_LIBRARY_PATH_64". This placeholder is an empty string on other operating systems.
%DLLPREFIX%	The default prefix of a `.dll` or `.so` file.	On UNIX, "lib". This placeholder is an empty string on Windows machines.
%DLLPRELOAD%	The name of the LD_PRELOAD environment variable for the platform.	On UNIX *LD_PRELOAD*. This placeholder is an empty string on Windows machines.
%DLLPRELOAD32%	The name of the LD_PRELOAD environment variable on 32-bit AIX systems.	On AIX, *LDR_PRELOAD*. This placeholder is an empty string on other machines.
%DLLPRELOAD64%	The name of the LD_PRELOAD environment variable on 64-bit AIX systems.	On AIX, *LDR_PRELOAD64*. This placeholder is an empty string on other machines.
%DP%	The path delimiter.	On Windows, ";". On UNIX, ":".
%DefaultAuditingDir%	The directory where Auditing temporary files are written. For optimum performance, this location should be on the server's local drive.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\Auditing. On UNIX, **<INSTALLDIR>**/sap_bobj/data/Auditing/.
%DefaultDataDir%	The temporary directory used by the Job Server.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\Data. On UNIX, **<INSTALLDIR>**/sap_bobj/data/.
%DefaultInputFRSDir%	The root folder of the Input File Repository Server.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input. On UNIX, **<INSTALLDIR>**/sap_bobj/data/frsinput.
%DefaultLoggingDir%	The location where the log files are stored.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\logging. On UNIX, **<INSTALLDIR>**/sap_bobj/logging.
%DefaultOutputFRSDir%	The root folder of the Output File Repository Server.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output. On UNIX, **<INSTALLDIR>**/sap_bobj/data/frsoutput.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%DefaultWorkingDir%	The working directory for 64-bit servers	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\win64_x64. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<platform>**.
%DefaultWorkingDir32%	The working directory for 32-bit servers.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\win32_x86. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/**<platform>**.
%EPM_LD_PRELOAD_ONCE%	The name of the LD_PRELOAD_ONCE environment variable for the platform.	$LD_PRELOAD_ONCE$
%EVENTSERVER_EXE%	The name of the executable for the Event Server.	On Windows, EventServer.exe. On UNIX, boe_eventsd.
%EXEEXT%	The default extension of executable files.	On Windows, .exe. This placeholder is unavailable on UNIX.
%EXEPATH%	The name of the environment variable on the computer on which SAP BusinessObjects Business Intelligence platform is installed that specifies the directories there the interpreter will search for executable files.	On Windows, "Path". On UNIX, "PATH".
%EnterpriseDir%	The location where 64-bit SAP BusinessObjects Business Intelligence platform is installed.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40.
%EnterpriseDir32%	The location where 32-bitSAP BusinessObjects Business Intelligence platform is installed.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40.
%ExternalJavaLibDir%	The folder where external, third-party Java libraries are located.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\java\lib\external. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/java/lib/external.
%FILESERVER_EXE%	The name of the executable for the File Server	On Windows, fileserver.exe. On UNIX, boe_filesd.
%HOARD_PATH%	The location of the memory manager.	By default, this is empty.
%HOARD_PRELOAD%	Specifies whether to preload the memory manager.	By default, this is empty.
%INSTALLROOTDIR%	The folder where 64-bit SAP BusinessObjects Business Intelligence platform is installed.	This value is specified during installation.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%INSTALLROOTDIR32%	The folder where 32-bit SAP BusinessObjects Business Intelligence platform is installed.	This value is specified during installation.
%IntroscopeAgentEnableInstrumentation%	Indicates whether instrumentation for Java servers using Introscope Agent Enterprise Manager is enabled.	Possible values are TRUE or FALSE, depending on whether Introscope Agent Enterprise Manager was enabled when SAP BusinessObjects Business Intelligence platform was installed.
%IntroscopeAgentEnterpriseManagerHost%	The Introscope Agent Enterprise Manager hostname to which instrumentation data is sent.	This value is specified during installation.
%IntroscopeAgentEnterpriseManagerPort%	The Introscope Agent Enterprise Manager port to which instrumentation data is sent.	This value is specified during installation.
%IntroscopeAgentEnterpriseManagerTransport%	The transport that is used when sending instrumentation data to the Introscope Agent Enterprise Manager. Allowed values are: • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through HTTP.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through HTTPS.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through SSL.	com.wily.isengard.postoffice-hub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	The class that is used when sending instrumentation data to the Introscope Agent Enterprise Manager through TCP.	com.wily.isengard.postoffice-hub.link.net.DefaultSocketFactory
%IntroscopeDir%	The folder where Introscope Agent Enterprise Manager is installed.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\java\wily. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/java/wily.
%JAVAW_EXE%	The name of the executable for the Java Virtual Machine that has no console window.	On Windows, `javaw.exe`. On UNIX, `java`.
%JAVA_EXE%	The name of the executable for the Java Virtual Machine.	On Windows, `java.exe`. On UNIX, `java`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%JOBSERVERCHILD_EXE%	The name of the executable for the Adaptive Job Server Child.	On Windows, `JobServerChild.exe`. On UNIX, `boe_jobcd`.
%JOBSERVER_EXE%	The name of the executable for the Adaptive Job Server.	On Windows, `JobServer.exe`. On UNIX, `boe_jobsd`.
%JdkBinDir%	The folder where the JDK binaries are located.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. On UNIX, **<INSTALLDIR>**`/sap_bobj/`**<PLATFORM>**`/sapjvm/bin`.
%JreBinDir%	The folder where the JRE binaries are located.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`. On UNIX, **<INSTALLDIR>**`/sap_bobj/`**<PLATFORM>**`/sapjvm/jre/bin`.
%JVM_ARCH_ENVIRONMENT%	Indicates whether the machine is running on the 32-bit or 64-bit JVM.	For 32-bit UNIX machines, the default value is "-d32". For 64-bit machines, the default value is "-d64". On Windows machines, this is an empty string.
%JVM_HEADLESS_MODE%	The command-line argument that specifies whether the JVM works in headless mode.	On Windows, -Djava.awt.headless=false. On UNIX, -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	The command-line parameters that specify what the JVM does when it encounters Out of Memory errors.	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	The command-line parameters that enable JVM extensions and set the JVM's instance number.	By default, this placeholder is empty.
%LANGUAGEPACKSDIR%	The folder where the deployment's language packs are installed.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\Languages`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/Languages/`.
%LANGUAGEPACKSDIR32%	The folder where the deployment's language packs are installed on 32-bit systems.	. On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\Languages`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/Languages/`.
%LSTDir%	The folder where LST configuration files are stored.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\conf\lst`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/conf/lst`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%MDAS_JVM_OS_STACK_SIZE%	Specifies the JVM stack-size for the Multidimensional Analysis Service.	By default, this placeholder is empty.
%NCSInstrumentLevelThreshold%	The threshold level of trace logging for the NCS library.	By default, this value is 0.
%PAGESERVER_EXE%	The name of the executable for the Crystal Reports 2013 Processing Server.	On Windows, `crproc.exe`. On UNIX, `boe_crprocd.bin`.
%PJSContainerDir%	The folder where APS Container JARS are located.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/java/pjs/container`.
%PJSServicesDir%	The folder where APS Service JARS are located.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/java/pjs/services`.
%Platform%	The operating system of the machine that SAP BI platform is running on.	The operating system of the machine that SAP BI platform is running on.
%Platform32%	The operating system of the machine that 32-bit SAP BI platform is running on.	The operating system of the machine that SAP BI platform is running on.
%RasBinDir%	The root folder of the Report Application Server.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/`**<PLATFORM>**`/ras`.
%SERVER_FRIENDLY_NAME%	The full name of the server.	The full name of the server.
%SERVER_NAME%	The full name of the server.	The full name of the server.
%SMDAgentHost%	The SMD Agent hostname to which instrumentation data is sent.	This value is specified during installation.
%SMDAgentPort%	The SMD Agent port to which instrumentation data is sent.	This value is specified during installation.
%TRACE_CONFIGFILE_INI%	The name and path of the `BO_Trace.ini` file.	On Windows, **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini`. On UNIX, **<INSTALLDIR>**`/sap_bobj/enterprise_xi40/conf/BO-trace.ini`.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Placeholder	Description	Default values
%WarFilesDir%	The location of web application files.	On Windows, **<INSTALLDIR>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps. On UNIX, **<INSTALLDIR>**/sap_bobj/enterprise_xi40/warfiles/webapps.
%WEBI_LD_PRELOAD%	The name of the LD_PRELOAD environment variable for the platform.	$LD_PRELOAD$
%WEBISERVER_EXE%	The name of the executable for the Web Intelligence Processing Server.	On Windows, wireportserver.exe. On UNIX, WIReportServer.
%WEBI_LD_PRELOAD_ONCE%	The name of the LD_PRELOAD_ONCE environment variable for the platform.	$LD_PRELOAD_ONCE$
%XCCACHE_EXE%	The name of the executable for the Dashboards Cache Server.	On Windows, xccache.exe. On UNIX. boe_xccached.
%XCPROC_EXE%	The name of the executable for the Dashboards Processing Server.	On Windows, xcproc.exe. On UNIX, boe_xcprocd.

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%*

Related Information

To view and edit the placeholders for a node [page 395]

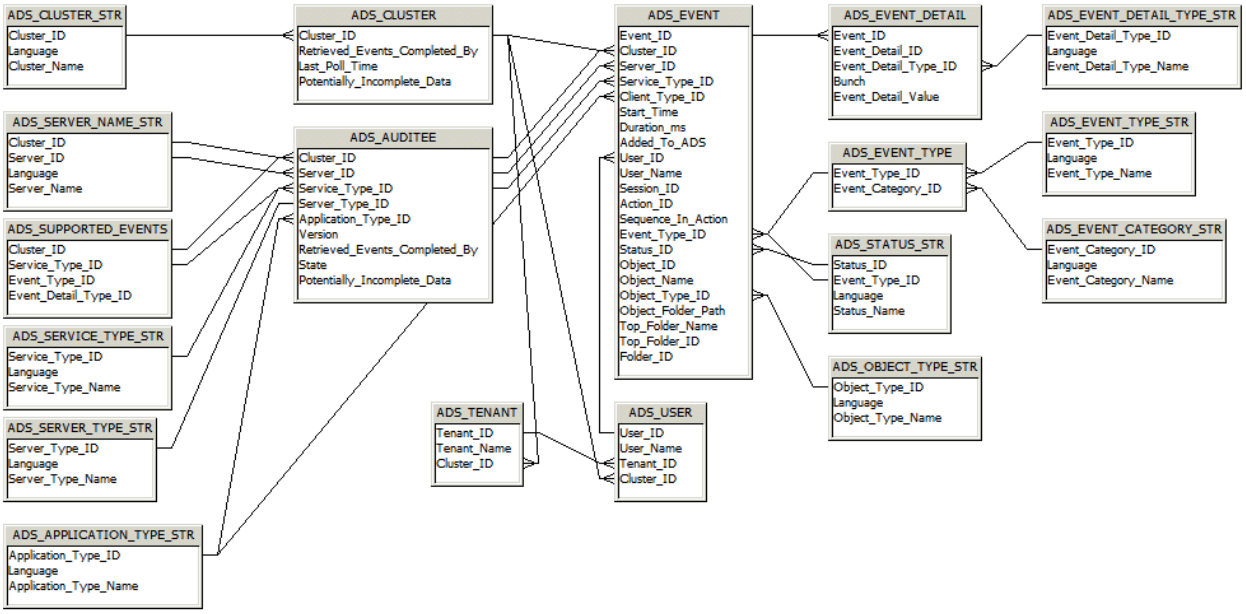
© 2015 SAP SE or an SAP affiliate company. All rights reserved.

33 Auditing Data Store Schema Appendix

33.1 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.

33.2 Schema diagram



33.3 Auditing Data Store Tables

ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 250:

Column Name	Type	Description
Application_Type_ID	Character (64)	The application-type CUID for the application.
Language	Character (10)	Code for the language in which the application type is recorded; for example **<EN>**, or **<DE>**.
Application_Type_Name	Character (255)	The text name of the application type; Crystal Reports or Web Intelligence for example.

ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Table 251:

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	The server-type CUID for the server that triggered the event.
Application_Type_ID	Character (64)	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS.
State	Integer	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	Shows if this auditee may have events that were not transferred to the ADS.

ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

Table 252:

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Column Name	Type	Description
Retrieved_Events_Completed_By	Datetime	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS.

ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

Table 253:

Column Name	Type	Description
Cluster_ID	Character (64)	A unique ID of the cluster.
Language	Character (10)	Code for the language setting for the cluster, for example, **<EN>**, or **<DE>**.
Cluster_Name	Character (255)	The name of the cluster.

ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

Table 254:

Column Name	Type	Description
Event_ID	Character (64)	A unique ID generated for the event.
Cluster_ID	Character (64)	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	• The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID. • Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID.
Client_Type_ID	Character (64)	Records the Client Type ID of the client that established the session.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Column Name	Type	Description
Start_Time	Datetime	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	Duration of operation in milliseconds.
Added_to_ADS	Datetime	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	The CUID of the user who performed the action.
User_Name	Character (255)	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.
Event_Type_ID	Integer	Type of event (View or Save, for example).
Status_ID	Integer	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	CUID of the object that the operation was performed on.
Object_Name	Character (255)	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded.
Top_Folder_ID	Character (64)	The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded.

ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

Table 255:

Column Name	Type	Description
Event_Category_ID	Integer	The event-category ID.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Column Name	Type	Description
Language	Character (10)	Code for the language that the event category name is recorded in; for example **<EN>**, or **<DE>**.
Event_Category_Name	Character (255)	The name of the event category.

ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

ADS_EVENT_DETAIL table

This table records event detail properties.

Table 256:

Column Name	Type	Description
Event_Detail_ID	Integer	GUID for the event detail.
Event_ID	Character (64)	Parent event GUID.
Event_Detail_Type_ID	Integer	Type of event detail.
Bunch	Integer	If the detail is part of a series, this is used to tie them together. For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of: • Prompt Name: Country • Prompt Value: USA Bunch 2 would consist of: • Prompt Name: State • Prompt Value: California • Prompt Value: Nevada
Event_Detail_Value	Character (long-text)	The value of the event detail.

ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Table 257:

Column Name	Type	Description
Event_Detail_ID	Integer	The event detail-type ID for the event detail.
Language	Character (10)	Code for the language that the event detail name is recorded in; for example **<EN>**, or **<DE>**.
Event_Detail_Type_Name	Character (255)	The text name of the event detail type.

ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

Table 258:

Column Name	Type	Description
Event_Type_ID	Integer	The unique identifier for the type of event.
Event_Category_ID	Integer	Category of event. For example, common, Web Intelligence, or Life-Cycle Management.

ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

Table 259:

Column Name	Type	Description
Event_Type_ID	Integer	The event-type ID for the event.
Language	Character (10)	Code for the language that the event category name is recorded in; for example **<EN>**, or **<DE>**.
Event_Type_Name	Character (255)	The text name of the event type; View or Logon for example.

ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

Table 260:

Column Name	Type	Description
Object_Type_ID	Character (64)	Object-type CUID of the object
Language	Character (10)	Code for the language that the object type name is recorded in; for example **<EN>**, or **<DE>**.
Object_Type_Name	Character (255)	Name of the object type.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Table 261:

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	The CUID of the server.
Language	Character (10)	Code for the language of the server name; for example **<EN>**, or **<DE>**.
Server_Name	Character (255)	The name of the server.

ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

Table 262:

Column Name	Type	Description
Service_Type_ID	Character (64)	The service-type or service-category CUID for the service.
Language	Character (10)	Code for the language the service-type name is recorded in, for example **<EN>**, or **<DE>**.
Service_Type_Name	Character (255)	The name of the service-type.

ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

Table 263:

Column Name	Type	Description
Status_ID	Integer	The numerical representation of the operation's status.
Event_Type_ID	Integer	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Code for the language that the event status is recorded in; for example **<EN>**, or **<DE>**.
Status_Name	Character (255)	A text description of the event's status; Succeeded or Failed, for example.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Table 264:

Column Name	Type	Description
Cluster_ID	Character (64)	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	CUID that identifies the type of event detail captured for that event (File Path, for example).

ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

Table 265:

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
Tenant_ID	Character (64)	The CUID of the tenant.
Tenant_Name	Character (255)	The name of the tenant.

ADS_USER Table

This table records the relationship between users and tenants.

Table 266:

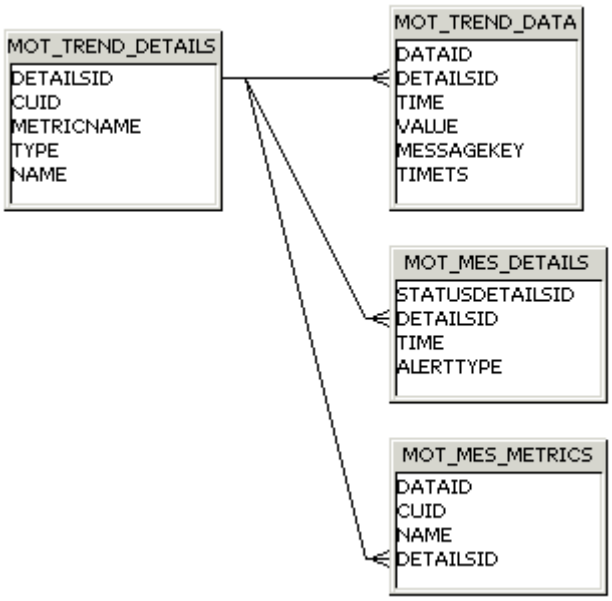
Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
User_ID	Character (64)	The CUID of the user.
User_Name	Character (255)	The name of the user.
Tenant_ID	Character (64)	The CUID of the tenant.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

34 Monitoring Database Schema Appendix

34.1 Trending database schema

The following Trending database diagram and table explanations show you the tables where the metric, probe, and watch data will be recorded and how these tables are related.



MOT_TREND_DETAILS

This table records information about managed entities, probes, and watches. For example, CUID and metric names.

Table 267:

Column Name	Type	Key	Description
DetailsId	INTEGER	Primary Key Autogenerated	
CUID	VARCHAR(64)	NA	CUID of the InfoObject that exposes the metric or is related to the metric
MetricName	VARCHAR(255)	NA	Name of the Metric
Type	VARCHAR(32)	NA	One of "Subscription", "ManagedEntityStatus", or "Probe"

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Column Name	Type	Key	Description
Name	VARCHAR(255)	NA	Name of the watch when the type is "ManagedEntityStatus". Otherwise, default to the same string as in Type, except in all capital letters; for example, "PROBE" or "SUBSCRIPTION".

MOT_TREND_DATA

This table records the trending data from metrics, watches, and probes. For example, metric value and time.

Table 268:

Column Name	Type	Key	Description
DataId	INTEGER	Primary Key Autogenerated	
DetailsId	INTEGER	Foreign key (from MOT_TREND_DETAILS)	
Time or TimeT	BIGINT or NUMBER or FIXED Unix Epoch date	NA	Time at which data was collected
Value	FLOAT or DOUBLE or NUMBER	NA	Value of the metric / subscription
MessageKey	VARCHAR(32)	NA	Error message key or null if successful. For Watch, it can also be either "watchEnabled" or "watchDisabled". It is a "key" because it is ultimately used to fetch localized messages before displaying the UI.
Ts	DATETIME or TIMESTAMP	NA	Time at which data is written to the database

MOT_MES_DETAILS

This table records the information about subscription breaches and alert delivery information. For example, breach time and alert delivery time.

Table 269:

Column Name	Type	Key	Description
StatusDetailsId	INTEGER	Primary Key Autogenerated	

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Column Name	Type	Key	Description
DetailsId	INTEGER	Foreign key (from MOT_TREND_DETAILS)	
Time	BIGINT or NUMBER Unix Epoch date	NA	Time at which data was collected
AlertType	SMALLINT or NUMBER	NA	Subscription notification delivery type (for example, email)

MOT_MES_METRICS

This table records information about watches and the metrics belonging to the watch equations. Every metric belonging to the watch will have one entry in this table.

Table 270:

Column Name	Type	Key	Description
DataId	INTEGER	Primary Key Autogenerated	
DetailsId	INTEGER	Foreign key (from MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	NA	CUID of the watch
Name	VARCHAR(255)	NA	Name of the watch

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

35 System Copy Worksheet Appendix

35.1 System copy worksheet

Table 271:

Property	Value
Cluster key.	
Names of the nodes.	
The machine name and the BI platform installation folder for each machine in the deployment.	
The BI platform administrator password.	
CMS database connections, the user names and passwords associated with those connections for each machine in the deployment.	
Auditing database connections, the user names and passwords associated with those connections for each machine in the deployment.	
For each machine in the deployment, details of any other database client connections for each machine in the source system used by universes and reports.	
For each machine in the deployment, database client types and versions.	
The version, support package, and patch level.	
The file store locations for every Input FRS and Output FRS in the deployment.	
If you plan to copy Promotion Management, the location of the Promotion Management database folder and Subversion folders.	
If you plan on copying the monitoring database, the monitoring database folder.	
The semantic layer folder path.	

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

www.sap.com/contactsap

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.
Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.
These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.
SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.
Please see http://www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.