

IBM® Cognos® 8 Planning

INSTALLATION AND CONFIGURATION GUIDE



Product Information

This document applies to IBM® Cognos® 8 Planning Version 8.4 and may also apply to subsequent releases. To check for newer versions of this document, visit the Cognos Software Services Web site (<http://support.cognos.com>).

Copyright

Copyright © 2008 Cognos ULC (formerly Cognos Incorporated). Cognos ULC is an IBM Company.

Portions of Cognos ULC software products are protected by one or more of the following U.S. Patents: 6,609,123 B1; 6,611,838 B1; 6,662,188 B1; 6,728,697 B2; 6,741,982 B2; 6,763,520 B1; 6,768,995 B2; 6,782,378 B2; 6,847,973 B2; 6,907,428 B2; 6,853,375 B2; 6,986,135 B2; 6,995,768 B2; 7,062,479 B2; 7,072,822 B2; 7,111,007 B2; 7,130,822 B1; 7,155,398 B2; 7,171,425 B2; 7,185,016 B1; 7,213,199 B2; 7,243,106 B2; 7,257,612 B2; 7,275,211 B2; 7,281,047 B2; 7,293,008 B2; 7,296,040 B2; 7,318,058 B2; 7,325,003 B2; 7,333,995 B2.

Cognos and the Cognos logo are trademarks of Cognos ULC (formerly Cognos Incorporated) in the United States and/or other countries. IBM and the IBM logo are trademarks of International Business Machines Corporation in the United States, or other countries or both. Other company, product, or service names may be trademarks or service marks of others.

While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. Cognos does not accept responsibility for any kind of loss resulting from the use of information contained in this document.

This document shows the publication date. The information contained in this document is subject to change without notice. Any improvements or changes to the information contained in this document will be documented in subsequent editions.

U.S. Government Restricted Rights. The software and accompanying materials are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to the restrictions in subparagraph (C)(1)(ii) of the Rights in Technical Data and Computer clause at DFARS 252.227-7013, or subparagraphs (C)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48CFR52.227 as applicable. The Contractor is Cognos Corporation, 15 Wayside Road, Burlington, MA 01803.

This document contains proprietary information of Cognos. All rights are reserved. No part of this document may be copied, photocopied, reproduced, stored in a retrieval system, transmitted in any form or by any means, or translated into another language without the prior written consent of Cognos.

Table of Contents

[Introduction](#) 9

Part 1: IBM Cognos 8 Planning

[What's New?](#) 13

[New Features in Version 8.4](#) 13

[Contributor Web Client](#) 13

[Upgrade](#) 13

[The More Documentation Page](#) 14

[Changed Features in Version 8.4](#) 14

[Packaging for IBM Cognos 8 Planning](#) 14

[Chapter 1: Components Used by IBM Cognos 8 Planning](#) 17

[Server Components](#) 17

[Modeling Components](#) 18

[Other Components](#) 19

Part 2: Planning Your Installation

[Chapter 2: Installation Options](#) 21

[Installing All Server Components on One Computer](#) 21

[Installing the Gateway on a Separate Computer](#) 23

[Installing the Planning Server and Content Manager on Separate Computers](#) 25

[Multiple Installations of Content Manager](#) 27

[Installing Multiple Planning Servers](#) 28

[Distributed Installation in a Small Environment](#) 28

[Distributed Installation in a Medium or Large Environment](#) 29

[Installing Administration Clients](#) 30

[Installing Framework Manager](#) 32

[Installing IBM Cognos 8 Planning with IBM Cognos 8 Business Intelligence](#) 34

[Chapter 3: Workflow for IBM Cognos 8 Planning](#) 37

[Prepare for Implementation](#) 37

[Install IBM Cognos 8 Planning](#) 37

[Configure IBM Cognos 8](#) 38

[Monitor Configuration Changes](#) 39

[Configure Security](#) 39

[Administer IBM Cognos 8](#) 40

[Chapter 4: Setting Up Your Environment](#) 41

[Recommendation - Review the Readme Before You Install](#) 41

[Review Supported Environments](#) 41

[Verify System Requirements](#) 42

[Set Up Database Connectivity for the Content Store Database](#) 43

[Set Up Database Connectivity for the Planning Store Database](#) 44

[Create the Content Store and Planning Store](#) 44

Set Up the Database Client	49
Configure Web Browsers	50
Configure the Router to Test Dispatcher Availability	52
Set Up the Data Source or Import Source Environment	52
Part 3: Installation and Configuration	
Chapter 5: Upgrading to IBM Cognos 8 Planning	55
Upgrading IBM Cognos 8 Business Intelligence	56
Choosing the Upgrade Tool	57
Planning the Upgrade	57
Review the Documentation	59
Recommendation - Assess Applications in the Source Environment	59
Recommendation - Perform a Trial Upgrade	60
Create the Test Environment	60
Plan Your Deployment	61
Create an Export Deployment Specification	62
Copy the Deployment Specification to the Test Environment	63
Import to the Test Environment	63
Recommendation - Test the Upgraded Content	65
Moving to the Production Environment	65
Upgrading Planning Administration Domains	67
Upgrading Planning Applications	67
Upgrade Analyst Security and Library Files	67
Upgrade Analyst Libraries, User Classes, Users, and Groups	67
Upgrading a Test or Development Environment	68
Upgrading From Versions 7.2, 7.3, or 8.1	68
Chapter 6: Installing and Configuring IBM Cognos 8 Planning on One Computer	71
Install IBM Cognos 8 Planning	71
Start IBM Cognos Configuration	73
Set Database Connection Properties for the Content Store	73
Set Database Connection Properties for the Planning Store	75
Configure Environment Properties	76
Enable Security	77
Configure the Web Server	78
Start the IBM Cognos 8 Planning Services	78
Uninstalling IBM Cognos 8	78
Uninstall IBM Cognos 8 on Windows	78
Chapter 7: Installing and Configuring IBM Cognos 8 Planning on Different Computers	81
Install and Configure Content Manager	83
Start IBM Cognos Configuration	84
Set Database Connection Properties for the Content Store	84
Configure Environment Properties for Content Manager	86
Enable Security	87
Start Content Manager	88
Test the Content Manager Installation	88
Install and Configure the Planning Server	88
Start IBM Cognos Configuration	90

Set Database Connection Properties for the Planning Store	90
Configure Environment Properties for the Planning Server	91
Configuring Role-based Planning Servers	92
Start the Planning Server	96
Install the Gateway	96
Start IBM Cognos Configuration	97
Configure Environment Properties for the Gateway	97
Configure the Web Server	98
Test the Gateway	99
Uninstalling IBM Cognos 8 Planning	99
Uninstall IBM Cognos 8 on Windows	99
Chapter 8: Installing the Planning Clients	101
Install IBM Cognos 8 Planning Administration Components	101
Default Settings for IBM Cognos 8 Planning - Administration Components	102
Configure Environment Properties for the Administration Components	102
Configuring Analyst Computers	103
Contributor Web Client	106
Installing and Configuring the Web Client	106
Set Installation Options the Contributor Web Client	107
Install the Contributor Web Client Using a Web Link	107
Install the Contributor Web Client Using a Command Line	108
Install the Web Client from the Planning Client Installation CD	109
Uninstall the Contributor Web Client	110
Install Contributor <i>for Microsoft Excel</i>	110
Install Framework Manager	111
Default Settings for Framework Manager	113
Configure Environment Properties for Framework Manager Computers	114
Configure a Source Control System	115
Install an Analyst Network Connection Point	116
Uninstall IBM Cognos 8	117
Chapter 9: Additional Configuration Options	119
Start IBM Cognos Configuration	119
Changing Default Configuration Settings	119
Change a URI	120
Configure Cryptographic Settings	122
Configure IBM Cognos 8 Components to Use IBM Cognos Application Firewall	124
Configure the Gateway to Use a Namespace	126
Enable and Disable Services	126
Specify Resources for the IBM Cognos 8 Service	127
Enable SSL on the Web Server	128
Configuring the SSL Protocol	129
Configure SSL for IBM Cognos 8	129
Set Up Shared Trust Between IBM Cognos Servers and Other Servers	132
Select and Rank Cipher Suites for SSL	133
Enable SSL on the Web Server	133
Changing the Gateway	135
Configure the Gateway for IBM Cognos Apache Web Server Module	135
Configure an IBM Cognos 8 UNIX Gateway for IBM Cognos 8 Planning	138

Configuring IBM Cognos 8 Planning to Work with Other IBM Cognos Products	139
Accessing Product Documentation in an Integrated Environment	139
Configuring IBM Cognos 8 Components to Use a Another Certificate Authority	140
Generate Keys and Certificate Signing Requests	140
Configure IBM Cognos 8 Components to Run Within Another Certificate Authority	144
Tuning Techniques for Improving Performance	144
Tuning a DB2 Content Store	145
Chapter 10: Configuring IBM Cognos 8 Components to Use an Authentication Provider	147
Disable Anonymous Access	148
Restrict User Access to the IBM Cognos Namespace	148
Configuring IBM Cognos 8 Components to Use Active Directory Server	149
Configure an Active Directory Namespace	149
Make Custom User Properties for Active Directory Available to IBM Cognos 8 Components	150
Enabling Secure Communication to the Active Directory Server	151
Include or Exclude Domains Using Advanced Properties	152
Enabling Single Signon Between Active Directory Server and IBM Cognos 8 Components	153
Configuring IBM Cognos 8 to Use IBM Cognos Series 7 Namespace	154
Configure an IBM Cognos Series 7 Namespace	154
Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace	155
Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos 8	155
IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in	156
Configuring IBM Cognos 8 to Use a Custom Authentication Provider	158
Configure a Custom Authentication Namespace	159
Hide the Namespace from Users During Login	159
Configuring IBM Cognos 8 Components to Use LDAP	160
Configure an LDAP Namespace	161
Configure an LDAP Namespace for Active Directory Server	162
Configure an LDAP Namespace for IBM Directory Server	165
Configure an LDAP Namespace for Novell Directory Server	167
Configure an LDAP Namespace for Sun Java System Directory Server	169
Make Custom User Properties for LDAP Available to IBM Cognos 8 Components	171
Enable Secure Communication to the LDAP Server	172
Enabling Single Signon Between LDAP and IBM Cognos 8 Components	173
Replace Operation	174
Configuring IBM Cognos 8 Components to Use eTrust SiteMinder	174
Configure a Netegrity SiteMinder Namespace	176
Enabling Secure Communication to the eTrust SiteMinder User Directory	177
Enable Single Signon Between eTrust SiteMinder and IBM Cognos 8	177
Protecting the IBM Cognos Web Alias	177
Hide the Namespace from Users During Login	177
Configuring IBM Cognos 8 Components to Use an NTLM Namespace	178
Configure an NTLM Namespace	178
Enable Single Signon Between NTLM and IBM Cognos 8 Components	179
Configuring IBM Cognos 8 to Use SAP	179
Configure an SAP Namespace	181
Enable Single Signon Between SAP and IBM Cognos 8	181

Test the Namespaces	182
Delete an Authentication Provider	182
Chapter 11: Configuring IBM Cognos 8 for an SAP Environment	185
Verify System Requirements	185
Set Access Permissions for Modeling and Reporting Access	186
Install and Configure IBM Cognos SAP Gateway Functions	188
Apply the SAP Gateway Functions	188
Install the IBM Cognos Compression Utility	189
Set Access Permissions for the IBM Cognos SAP Gateway Functions	189
Chapter 12: Configuring Portal Services	193
Specify the Location of the Applications.xml File	193
Configuring Security for Portal Services	194
Disable Anonymous Access to IBM Cognos 8 Components	194
Enable Single Signon Using Shared Secret	195
Enable Single Signon for SAP EP with the SAP Logon Ticket	200
Enable Single Signon for SAP EP with User Mapping	201
Enable Secure Communication Between SAP EP and IBM Cognos 8 Components	202
Enable Single Signon for WebSphere Portal Using the Application Server	202
Enable Single Signon for BEA ALUI Portal Using Basic Authentication	202
Enable Single Signon for BEA ALUI Portal Using SiteMinder	203
Chapter 13: Setting Up an Unattended Installation and Configuration	205
Set Up an Unattended Installation	205
Set Up an Unattended Configuration	208
Chapter 14: Setting Up the Samples for Contributor	211
Install Sun Java Systems Directory Server	211
Import the Sample Authentication Data	211
Configure IBM Cognos 8 Planning to Use Your Sun Java System Directory Server	212
Configure Contributor Administration	213
GO Contributor Sample	213
Create Contributor Applications	217
Recommended Cube Settings	218
Part 4: Troubleshooting	
Chapter 15: Troubleshooting	223
Log Files	223
Problems Starting IBM Cognos 8	225
CFG-ERR-0106 Error When Starting the IBM Cognos 8 Service in IBM Cognos Configuration	226
Unable to Start the IBM Cognos 8 Service Because the Port is Used by Another Process	227
IBM Cognos BI Server Not Available When Starting IBM Cognos 8	228
Cannot Log On to a Namespace When Using IBM Cognos Connection (PRS-CSE-1255 Error)	232
IBM Cognos 8 Services Fail to Restart After a Network Outage	232
No Warning That Installing a Later Version of IBM Cognos 8 Will Automatically Update the Earlier Version of the Content Store	232
Content Manager Error When Starting IBM Cognos 8	233

The Page Cannot Be Found When Starting IBM Cognos 8 in Windows 2003	233
The Page Is Not Shown When Opening a Portal After Installing IBM Cognos 8	233
DPR-ERR-2058 Error Appears in Web Browser When Starting IBM Cognos 8	233
DPR-ERR-2022 Error Appears in Web Browser When Starting IBM Cognos 8	235
Application Server Startup Script Fails	235
Permission Problems Using Contributor Administration or Analyst	235
Problems Integrating IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning	236
Page Not Found Error When Trying to Open Analysis Studio	236
Failed to Load the Pluggable Shared Library When Using Analysis Studio	236
Problems Using Contributor Administrator Caused by Incorrect Database Configuration	236
Problems Creating an Application in an SQL Environment	236
Problems Creating an Application in a DB2 Environment	237
Problems Importing Data in an SQL Environment	237
Problems Running Go to Production in an SQL Environment	237
Problems Creating a Module in Framework Manager Using a SAP BW Data Source	237
The BAP-ERR-0002 BAPI Error	237
The BAP-ERR-0002 BAPI Authorization Error for Function Group RSOB	238
The BAP-ERR-0002 BAPI Authorization Error for RFC_READ_TABLE	238
Authorization Error for Component	238
Authorization Error for InfoCube	238
Authorization Error for Hierarchy	238
Authorization Error for Temporary File	239
Authorization Errors Using the IBM Cognos SAP Gateway	239
Unable to Identify SAP Permissions Required	239
Unable to Identify SAP BW Version and Corrections	239
Error Messages in SAP Log When Using Data Manager Connector for SAP R/3	240
Fact Table Does Not Include Any Data	240
Glossary	241
Index	247

Introduction

This document is intended for use with IBM Cognos 8 Planning. It contains instructions for installing, upgrading, configuring, and setting up samples.

IBM Cognos 8 Planning provides the ability to plan, budget, and forecast in a collaborative, secure manner. The major components are Analyst and Contributor.

IBM Cognos 8 Planning - Analyst

Analyst is a flexible tool used by financial specialists to define their business models. These models include the drivers and content required for planning, budgeting, and forecasting. The models can then be distributed to managers using the Web-based architecture of IBM Cognos 8 Planning - Contributor.

IBM Cognos 8 Planning - Contributor

Contributor streamlines data collection and workflow management. It eliminates the problems of errors, version control, and timeliness that are characteristic of a planning system solely based on spreadsheets. Users have the option to submit information simultaneously through a simple Web or *Microsoft Excel*® interface. Using an intranet or secure Internet connection, users review only what they need to review and add data where they are authorized.

For more information about using this product, visit the Cognos Software Services Web site (<http://support.cognos.com>).

Best Practices for IBM Cognos 8 Planning

The Cognos Innovation Center™ for Performance Management provides a forum and Performance Blueprints that you can use to discover new ideas and solutions for finance and performance management issues. Blueprints are pre-defined data, process, and policy models that incorporate best practice knowledge from customers and the Cognos Innovation Center. These Blueprints are free of charge to existing customers or Platinum and Gold partners. For more information about the Cognos Innovation Center or the Performance Blueprints, visit <http://www.cognos.com/innovationcenter>.

Audience

To use this guide, you should be familiar with

- planning concepts
- database and data warehouse concepts
- security issues
- basic Windows administration skills
- the existing server environment and security infrastructure in your organization

Related Documentation

Our documentation includes user guides, getting started guides, new features guides, readmes, and other materials to meet the needs of our varied audience. The following documents contain related information and may be referred to in this document.

Note: For online users of this document, a Web page such as **The page cannot be found** may appear when clicking individual links in the following table. Documents are made available for your particular installation and translation configuration. If a link is unavailable, you can access the document on the Cognos Software Services Web site (<http://support.cognos.com>). Logon credentials are available either from your administrator or by request from cogcsslo@ca.ibm.com.

Document	Description
IBM Cognos 8 Planning Quick Start Installation and Configuration Guide	Installing and configuring IBM Cognos 8 Planning on a single computer using default settings for use in a test or small production environment
IBM Cognos 8 Administration and Security Guide	Managing servers, security, reports, and Portal Services; setting up IBM Cognos samples; and customizing IBM Cognos 8
IBM Cognos 8 Planning Architecture and Deployment Guide	Planning the IBM Cognos 8 planning architecture, developing installation strategies, including security considerations, and optimizing performance
IBM Cognos Configuration User Guide	Using IBM Cognos Configuration to configure IBM Cognos 8
IBM Cognos 8 Troubleshooting Guide	Helping administrators to quickly identify and solve problems
IBM Cognos 8 Planning - Contributor Administration Guide	Extending the Functionality of IBM Cognos 8 Planning - Contributor

Finding Information

To find the most current product documentation, including all localized documentation, access the Cognos Software Services Web site (<http://support.cognos.com>). Click the **Documentation** link to access documentation guides. Click the **Knowledge Base** link to access all documentation, technical papers, and multimedia materials.

Product documentation is available in online help from the **Help** menu or button in IBM Cognos products. You can also download documentation in PDF format from the Cognos Software Services Web site.

You can also read PDF versions of the product readme files and installation guides directly from IBM Cognos product CDs.

Using Quick Tours

Quick tours are short online tutorials that illustrate key features in IBM Cognos product components. To view a quick tour, start IBM Cognos Connection and click the **Quick Tour** link in the lower-right corner of the Welcome page.

Getting Help

For more information about using this product or for technical assistance, visit the Cognos Software Services Web site (<http://support.cognos.com>). This site provides product information, services, user forums, and a knowledge base of documentation and multimedia materials. To log a Service Request, go to IBM Cognos Insight! at <http://support.cognos.com/en/support/insight>. For general inquiries, contact your local Cognos Software Services office. Contact information can be found at <http://support.cognos.com/en/support/about/contact.html>. For information about education and training, click the **Training** link.

Printing Copyright Material

You can print selected pages, a section, or the whole book. You are granted a non-exclusive, non-transferable license to use, copy, and reproduce the copyright materials, in printed or electronic format, solely for the purpose of operating, maintaining, and providing internal training on IBM Cognos software.

What's New?

This section contains a list of [new](#) and [changed](#) features for this release. It will help you plan your upgrade and application deployment strategies and the training requirements for your users.

For information about new features for this release, see the *New Features Guide*.

To review an up-to-date list of environments supported by IBM Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the Cognos Global Customer Services Web site (<http://support.cognos.com>).

New Features in Version 8.4

Listed below are new features since the last release. Links to directly-related topics are included.

Contributor Web Client

Administrators can install the new [Contributor Web Client](#) or the original client, which is now called the [Classic Contributor Web client](#).

Administrators use the [Contributor Administration Console](#) to set options for downloading, installing, and updating the Contributor Web Client.

Depending on the options the administrator sets, either an administrator or a Contributor user can install the Web Client.

Installation Options for the Contributor Web Client

An administrator or Contributor users can install this Web client.

- An administrator can install the Contributor Web Client for a single user or all users by [using a command line to install](#) the IBM Cognos 8 Planning 8.4 Client Framework, and the IBM Cognos 8 Contributor 8.4.

Administrators can also install this client from the [IBM Cognos 8 Planning Client installation CD](#).

- A Contributor user can install the Web client by [clicking a Web link](#) on their Workflow page.

Installation Options for the Classic Contributor Web Client

Administrators can install the Classic client from the [IBM Cognos 8 Planning Client installation CD](#), or by [clicking a Web link](#).

Upgrade

Use the Deployment Wizard when you upgrade from Planning version 8.2 and above.

Since Planning version 8.4 is a major upgrade, we recommend that you create a new environment, starting with a clean content store. For more information, see [Upgrading to IBM Cognos 8 Planning](#).

The following are supported for upgrading to Planning 8.4:

Planning Item	Version
Planning Administration Domain Datastore	7.3, 8.1
Application Datastore	7.2, 7.3, 8.1
Deployment archives	8.2, 8.3

Depending on your version, you can upgrade the entire Planning Application Database or you can upgrade individual applications.

To determine which upgrade tool you need according to the version of Planning you currently have installed, see ["Choosing the Upgrade Tool" \(p. 57\)](#).

The More Documentation Page

Users that have administrator privileges can quickly access the **More Documentation** link from the **Help** menu in **Cognos Connection**. This provides administrators with a convenient way to quickly access documentation after Planning is installed.

They type of books that appear on the **More Documentation** page are

- Readmes
- Architecture and Deployment Guides
- Installation and Configuration Guides
- Administration and Portal Documentation

The documentation is only relevant to administrators, and is not associated with the user interface.

Changed Features in Version 8.4

Listed below are changes to features since the last release. Links to directly-related topics are included.

Packaging for IBM Cognos 8 Planning

The Contributor for Microsoft Excel CD is no longer available. The IBM Cognos Planning package now provides all installation components on three CDs instead of four. The following table lists each CDs and its installation components.

Note: The components on the Planning Server Components CD have not changed.

CD	Component
Planning Server Components	<ul style="list-style-type: none"> • Planning Server • Content Manager • Planning Gateway • Analyst UNC Connection Point
Planning Administration	<ul style="list-style-type: none"> • Analyst • Analyst for Microsoft Excel • IBM Cognos Planning Manager • Contributor Administration Console
Planning Client	<ul style="list-style-type: none"> • Planning Classic Client • Planning Client • Contributor for Microsoft Excel

What's New?

Chapter 1: Components Used by IBM Cognos 8 Planning

IBM Cognos 8 Planning uses both Windows- and Web-based components to provide planning solutions for budgeting and forecasting in a collaborative and secure manner. IBM Cognos 8 Planning uses a modelling tool to define the content required for planning, budgeting, and forecasting, and uses a Web-based architecture to distribute plans and allow users to input contributing data.

IBM Cognos 8 Planning uses standard IBM Cognos 8 components for security and distributing plans. IBM Cognos 8 Planning can be integrated in your existing IBM Cognos 8 environment.

IBM Cognos 8 Planning integrates easily into your existing infrastructure by using resources that are in your environment, such as a database for the content store and planning store or a security provider for authentication.

Server Components

Server components provide the user interfaces for distributing plans and contributing data, as well as the server functionality for routing and processing user requests. Server components include the following tools:

IBM Cognos 8 Planning - Contributor

IBM Cognos 8 Planning - Contributor streamlines data collection and workflow management. It eliminates the problems of errors, version control, and timeliness that characterize decentralized planning processes. Organizations can easily engage thousands of people in the planning process, collecting data from managers and staff across divisions and across geographies as well as from resellers, suppliers, and customers worldwide.

IBM Cognos 8 Planning - Contributor Administration

IBM Cognos 8 Planning - Contributor Administration enables administrators to publish an Analyst business model to the Web, manage access settings and model distribution, and configure the user's view of the model.

IBM Cognos 8 Planning - Manager

Use IBM Cognos 8 Planning - Manager to design reports using data stored in Analyst. Choosing this option installs IBM Cognos Planning - Manager on its own. You can select this if you do not want users to have direct access to Analyst. You must configure users' security to attain this.

Note: If you choose this option on its own, Analyst is also installed, but it is only accessible through objects in an IBM Cognos Planning - Manager report.

IBM Cognos Connection

IBM Cognos Connection is a Web portal provided with IBM Cognos 8, providing a single access point to the corporate data available for its products. It provides a single point of entry for querying,

analyzing, and organizing data, and for creating reports, scorecards, and events. Users can run all their Web-based IBM Cognos 8 applications through IBM Cognos Connection. Other business intelligence applications, and URLs to other applications, can be integrated with IBM Cognos Connection.

IBM Cognos Viewer

IBM Cognos Viewer is a portlet in which you can view and interact with any type of published IBM Cognos content. It is accessible through IBM Cognos Connection and any existing enterprise portal.

Event Studio

In Event Studio, you set up agents to monitor your data and perform tasks when business events or exceptional conditions occur in your data that must be dealt with. When an event occurs, people are alerted to take action. Agents can publish details to the portal, deliver alerts by email, run and distribute reports based on events, and monitor the status of events. For example, a support call from a key customer or the cancellation of a large order may trigger an event, sending an email to the appropriate people.

IBM Cognos Configuration

IBM Cognos Configuration is a tool that you use to configure IBM Cognos 8, and to start and stop its services.

Gateway

Web communication in IBM Cognos 8 is typically through gateways, which reside on one or more Web servers. A gateway is an extension of a Web server program that transfers information from the Web server to another server.

Gateways are often CGI programs, but may follow other standards, such as Internet Server Application Program Interface (ISAPI) and Apache Modules (apache_mod).

Content Manager

Content Manager is the IBM Cognos 8 service that manages the storage of customer application data, including security, configuration data, models, metrics, report specifications, and report output. Content Manager is needed to publish packages, retrieve or store report specifications, manage scheduling information, and manage the IBM Cognos namespace.

Content Manager stores information in a content store database.

Composite Information Server

Composite Information Server provides access to additional data sources such as LDAP, JDBC, Open XML and WSDL, and improves performance when querying data from different data sources.

Modeling Components

Modeling components model data within data sources to define the content required for planning, budgeting, and forecasting. Modeling components include the following tools:

IBM Cognos 8 Planning - Analyst

IBM Cognos 8 Planning - Analyst is both a stand-alone desktop analysis tool and the tool used to create the plans to distribute using the Web-based architecture of Contributor. Use Analyst to establish the structure that defines the key drivers and content required for planning, budgeting, and forecasting, and the distribution of templates to managers.

IBM Cognos 8 Planning - Analyst *for Microsoft Excel*

Use IBM Cognos 8 Planning - Analyst *for Microsoft Excel* to create a connection between the data held in Analyst and the view in Microsoft Excel. You can then create and transfer workbook data to and from the Analyst database.

Framework Manager

Framework Manager is the IBM Cognos 8 modeling tool for creating and managing business-related metadata for use in IBM Cognos 8 analysis and reporting. Metadata is published for use by reporting tools as a package, providing a single, integrated business view of any number of heterogeneous data sources.

Other Components

In addition to the tools provided with IBM Cognos 8, it requires the following components that are created using other resources.

Content Store

The content store is a relational database that contains data that IBM Cognos 8 Planning needs to operate, such as published plans, and the packages that contain them; connection information for data sources; information about the external namespace, and the IBM Cognos namespace itself. The relational database must be from a supported vendor.

Design models and log files are not stored in the content store.

The IBM Cognos 8 service that uses the content store is named Content Manager.

Planning Store

The planning store contains macros, links, access rights, system settings, and application linking information for your planning applications.

The planning store can be the same database as the content store or can be a separate database.

Communicating with the planning store is done using the object linking and embedding database (OLE DB) API.

Chapter 2: Installation Options

Before implementing IBM Cognos 8, decide how you will install and configure it to provide optimal performance. The choices that produce the best performance depend on your requirements, resources, and preferences.

When you assess your installation options for IBM Cognos 8, you must consider whether you are installing the product for the first time or upgrading. For information, see ["Upgrading to IBM Cognos 8 Planning" \(p. 55\)](#).

When you install IBM Cognos 8, you specify where to install the gateways, planning servers, and Content Manager. You can install all IBM Cognos 8 components on one computer, or distribute them over a network. You must also install the IBM Cognos 8 Planning administration clients, including Analyst Administration and Contributor Administration, and the Analyst and Contributor user clients, Contributor for Microsoft Excel, and Contributor Web client.

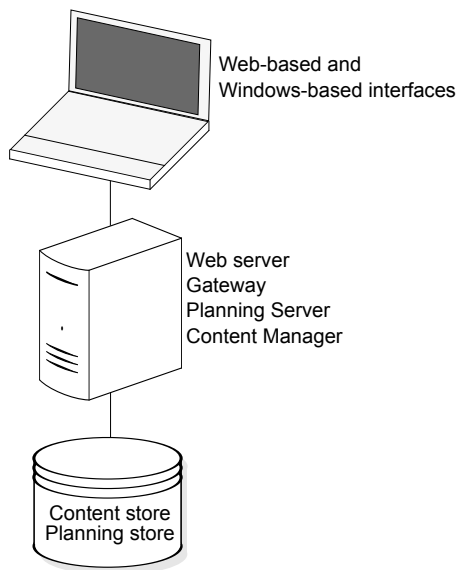
For advanced modeling and for use with Event Studio, you can install Framework Manager, the metadata modeling application. Framework Manager also provides additional data source access for IBM Cognos 8 Planning applications.

IBM Cognos 8 Planning is compatible with other IBM Cognos products. If your environment includes other IBM Cognos products, consider how IBM Cognos 8 Planning will fit into that environment.

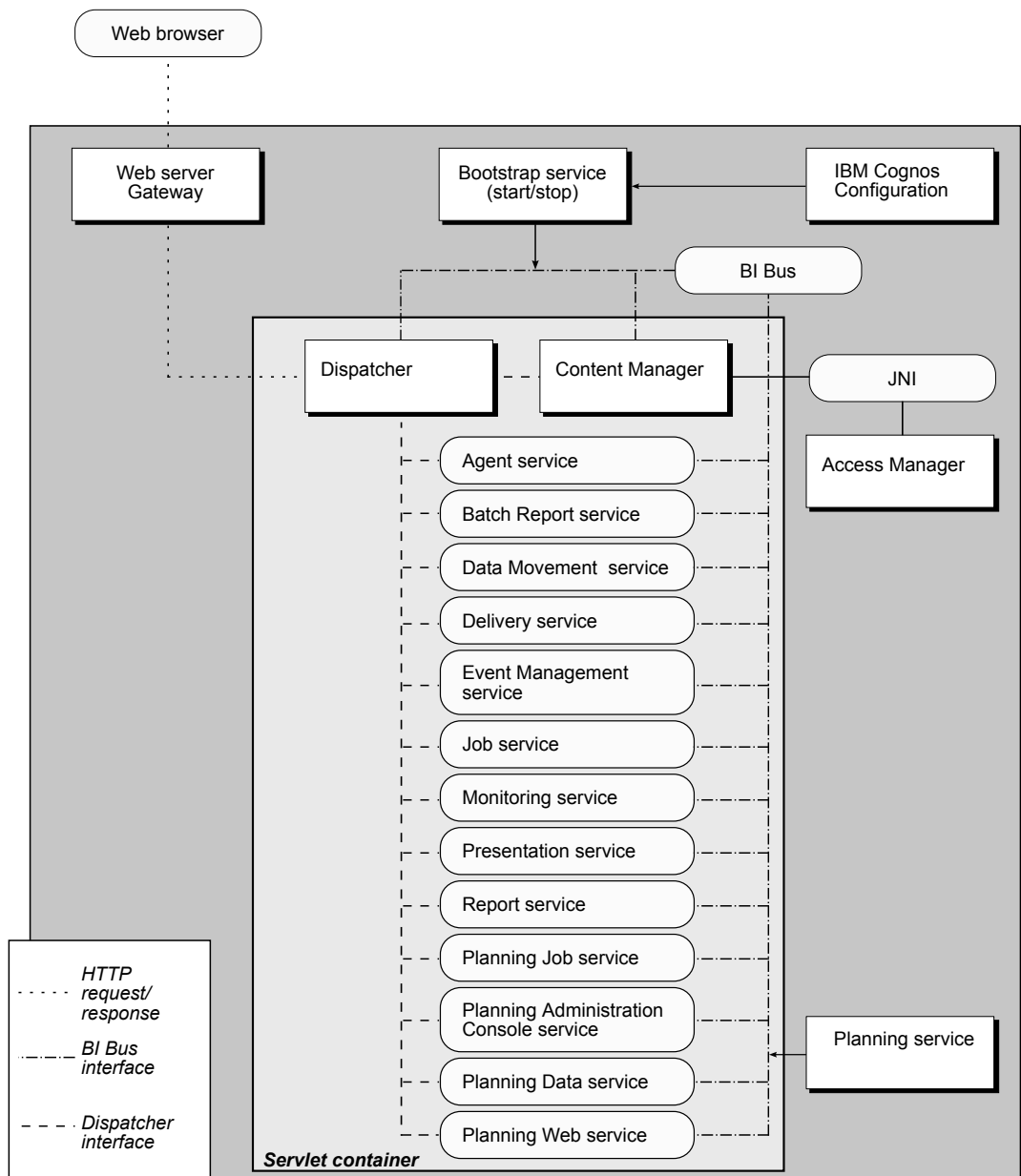
Installing All Server Components on One Computer

Install all server components on one computer only for proof of concept or in demonstration environments where the user load is small. Because the gateway must be located with the Web server, the single computer must also be running a Web server.

In the following diagram, all server components are installed on one computer, and the client applications are installed on another.



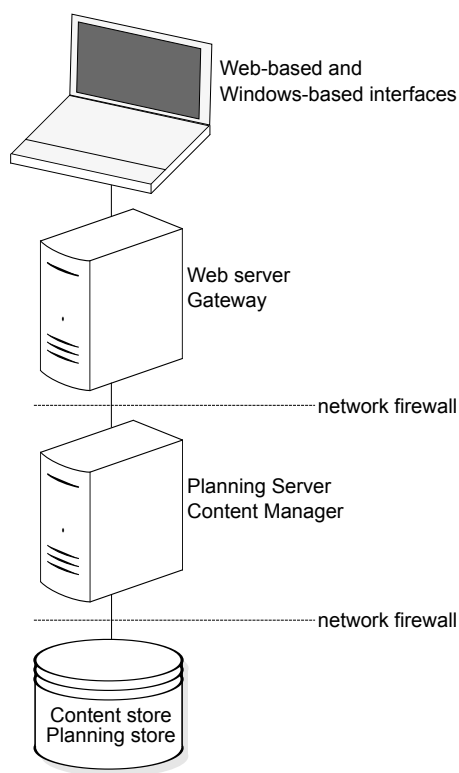
The following diagram provides a more detailed view of an IBM Cognos 8 installation in which all server components are installed on a single computer.



Installing the Gateway on a Separate Computer

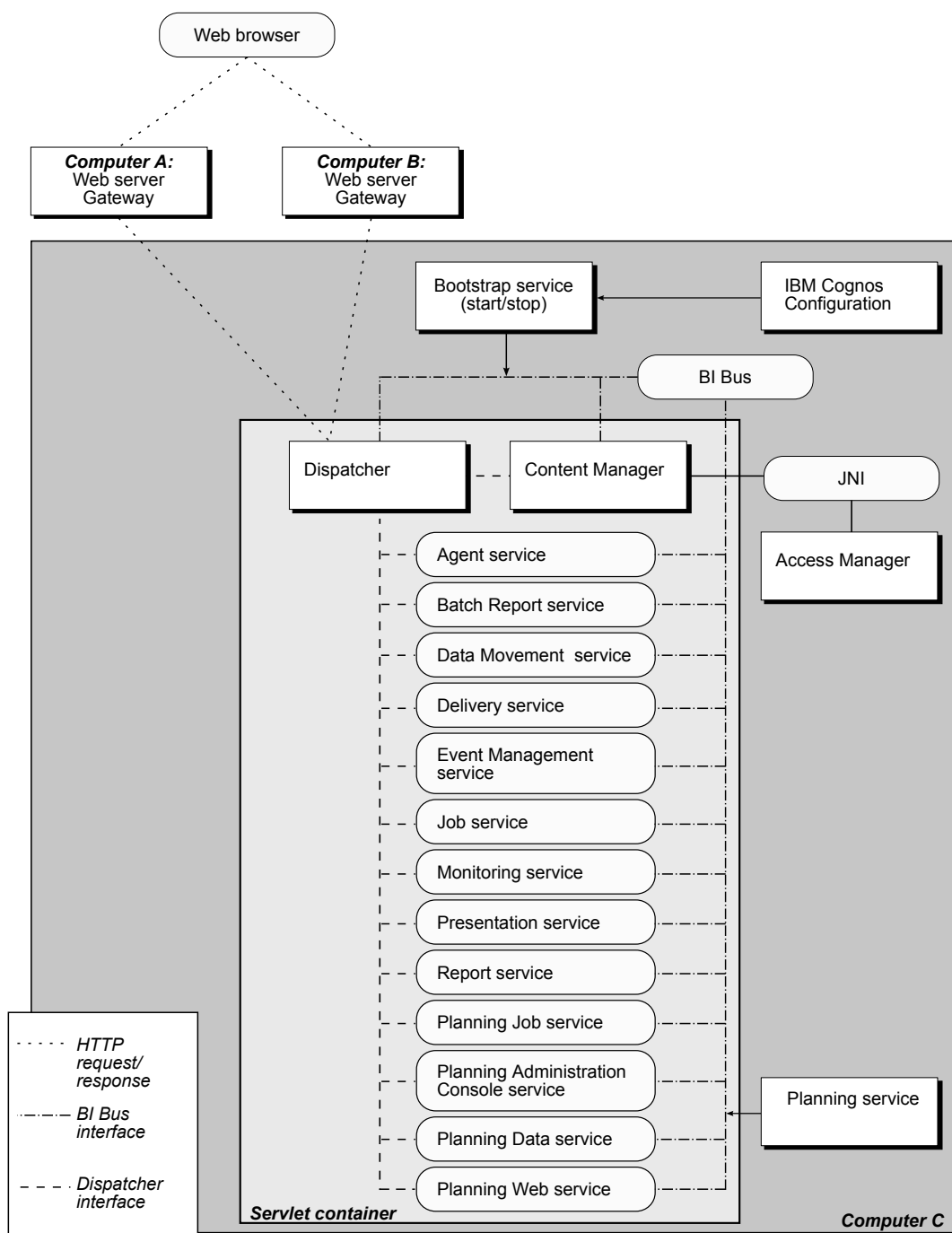
You can install the gateway and a Web server on one computer, and install the remaining IBM Cognos 8 components on other computers. If you have a Web farm, you may want to install an IBM Cognos 8 gateway on each Web server. Using multiple Web servers to manage incoming requests provides better service.

If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of processing may be required if you have a network firewall between the Web server and your Planning Server computers, as shown in the following diagram.



If you are installing into an environment with other IBM Cognos products, and you are using the same content store, we recommend that you either use the same gateway or install the gateway components of each product into the install locations of your other product's gateway. If you use separate gateways while sharing the content store, a `Page Not Found` error will appear when you use one product's component from the other product's gateway. For example, `Page Not Found` appears when you try to open Analysis Studio from the IBM Cognos 8 Planning gateway.

The following diagram provides a more detailed view of an installation in which the gateway is on a separate computer from other IBM Cognos 8 components. In this example, two Web servers are used, each with a gateway.

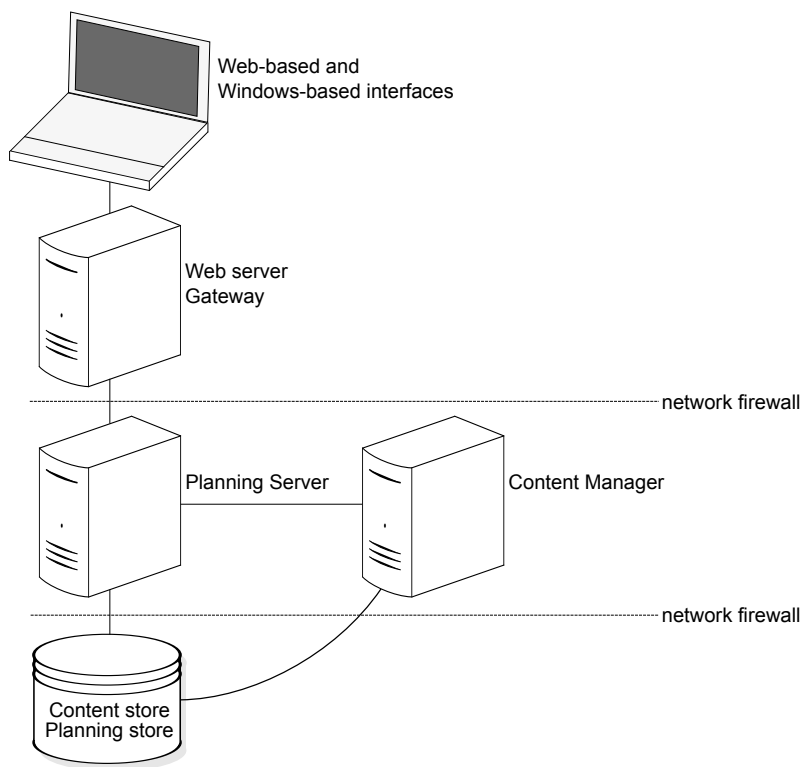


Installing the Planning Server and Content Manager on Separate Computers

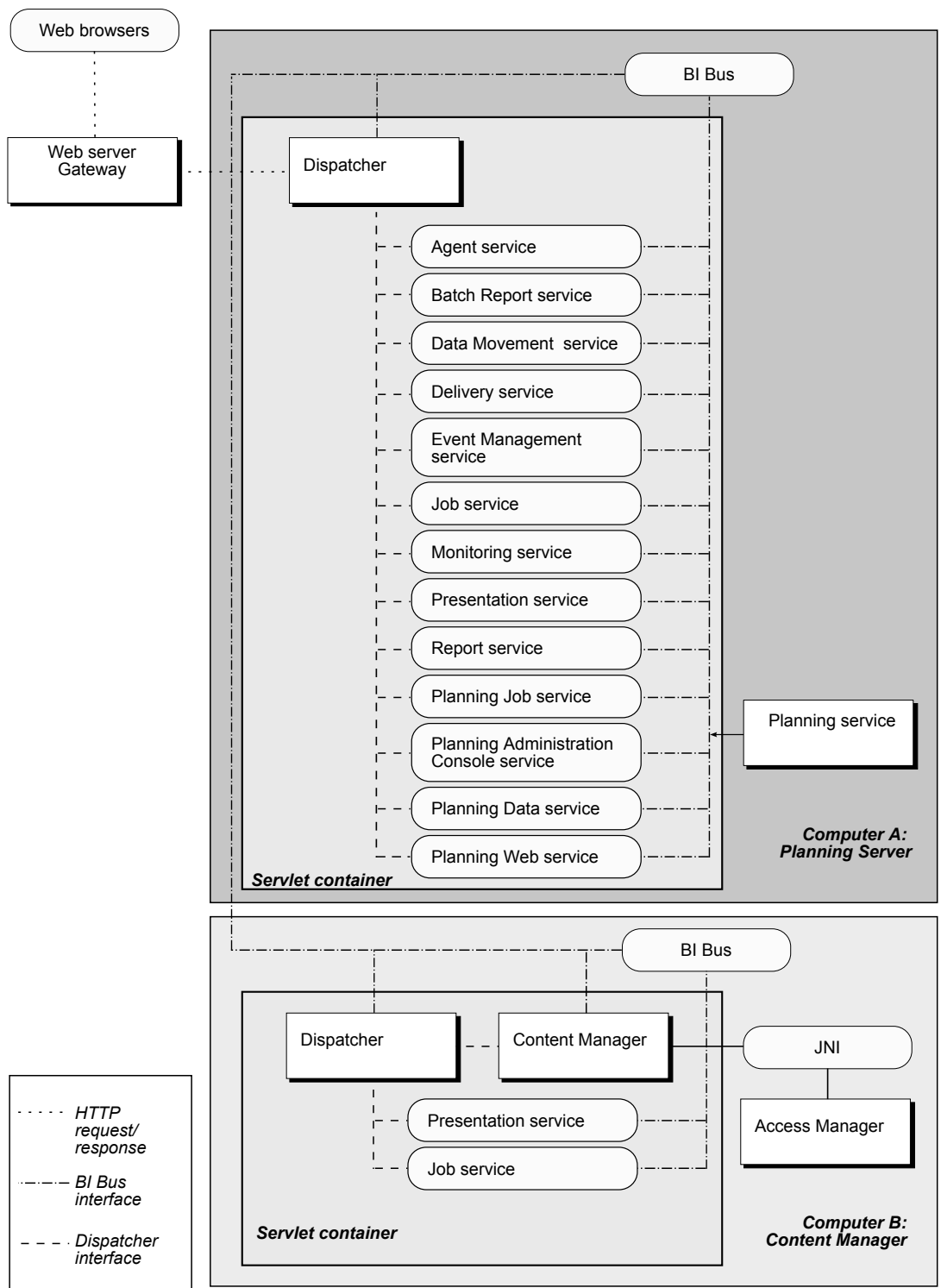
Installing the Planning Server on a separate computer from Content Manager can improve performance, availability, and capacity. This strategy is useful when

- your content store contains sensitive information
Data is then stored in the data tier with your security information.
- large volumes of data are managed by Content Manager

You can improve IBM Cognos 8 scalability by increasing the processor size on which Content Manager is installed.



The following diagram shows a more detailed view of an IBM Cognos 8 Planning installation in which separate computers are used for the Planning Server and Content Manager. Although this example shows only one installation of a Planning Server, your IBM Cognos 8 environment can include multiple Planning Server computers.



Multiple Installations of Content Manager

Your installation may include more than one Content Manager, each on a different computer. In this scenario, one Content Manager computer is active and one or more Content Manager computers are on standby. The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

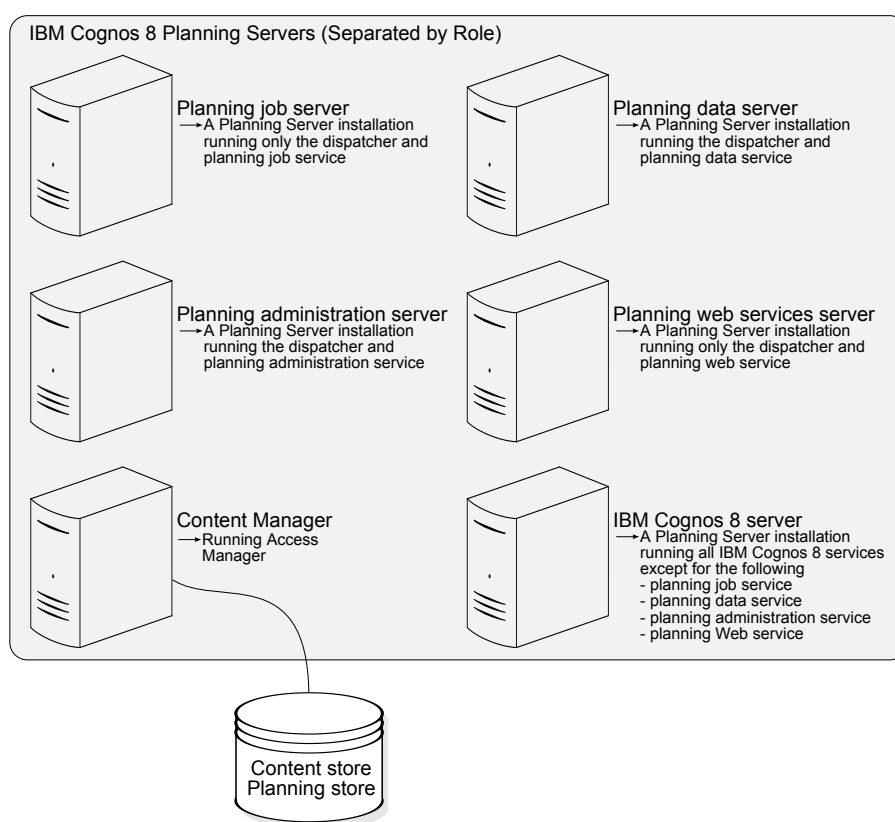
When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

Installing Multiple Planning Servers

To improve scalability in an environment that serves many users, you can install the Planning Server component on multiple computers dedicated to processing incoming requests. This strategy distributes and balances loads among the computers, and provides better accessibility, throughput, and failover support than installing on a single computer.

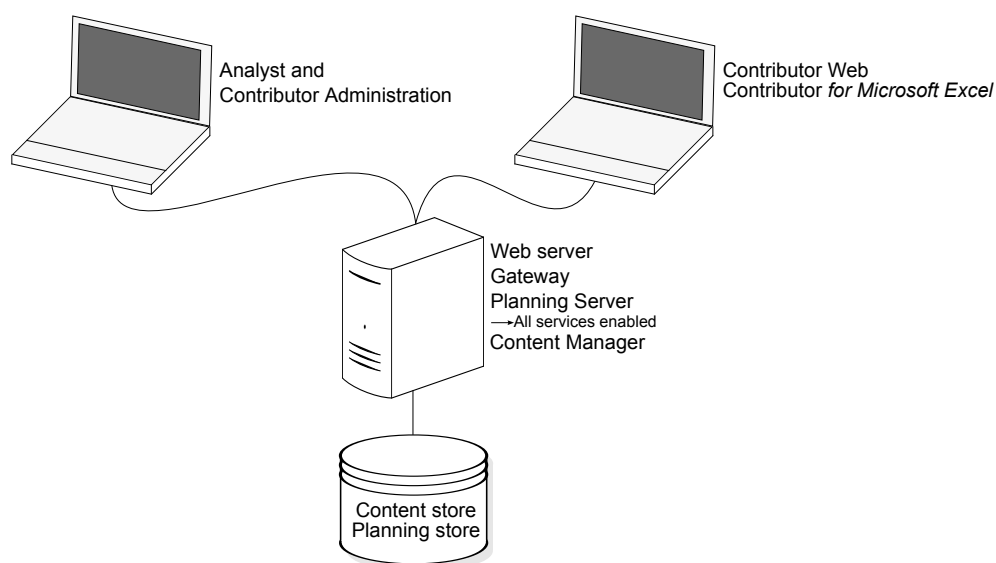
By distributing the Planning Server component you can set up role-based Planning Server computers. For more information, see ["Configuring Role-based Planning Servers" \(p. 92\)](#).

The following diagram shows an environment with each of the Planning Server roles on a separate computer, and one Planning Server running all the other IBM Cognos 8 services.



Distributed Installation in a Small Environment

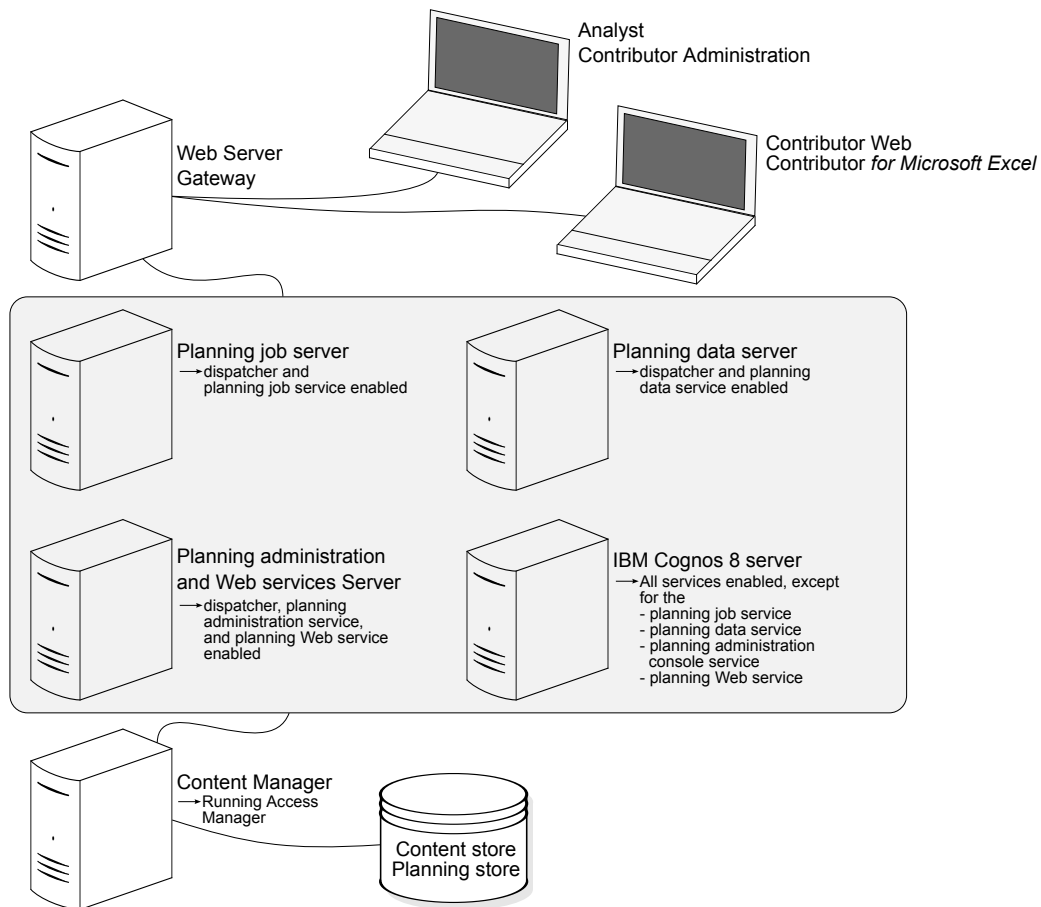
In a small environment, such as a proof of concept or demonstration environment, you can install all the server components on the same computer, and the server computer can run all the IBM Cognos 8 Planning services.



Distributed Installation in a Medium or Large Environment

In a medium-sized environment, you can distribute the Planning services among different servers to improve performance.

For example, you can separate the planning job service and planning data service onto different computers, the planning Web service and planning administration service can be on another computer, and the other IBM Cognos 8 services can be running on yet another computer. The Content Manager and gateway can also be on different computers.



To provide more stability and predictability, distribute your planning servers, if possible. If each service is isolated, it is not affected by the high usage of other services.

As additional computers become available, we recommend that you assign them to a dedicated role, in the following order:

- ☐ Specify that the first available computer run only the planning data service.
- ☐ Specify that the next available computer run only the planning job service.
- ☐ Specify that the next available computer run only the Content Manager service.
- ☐ Specify that the next available computer run only the gateway and planning Web service.

In a large environment, you can add servers to increase the number of planning job service computers and planning data service computers to meet your production needs. You can also run the planning Web service and planning administration service on separate Planning Server computers. For more information, see the IBM Cognos 8 Planning *Architecture and Planning Guide*.

Installing Administration Clients

You can install the administration clients on the same computer as the Planning Server components, or on a separate computer. Also, you can install each client independently.

The administration clients include the following:

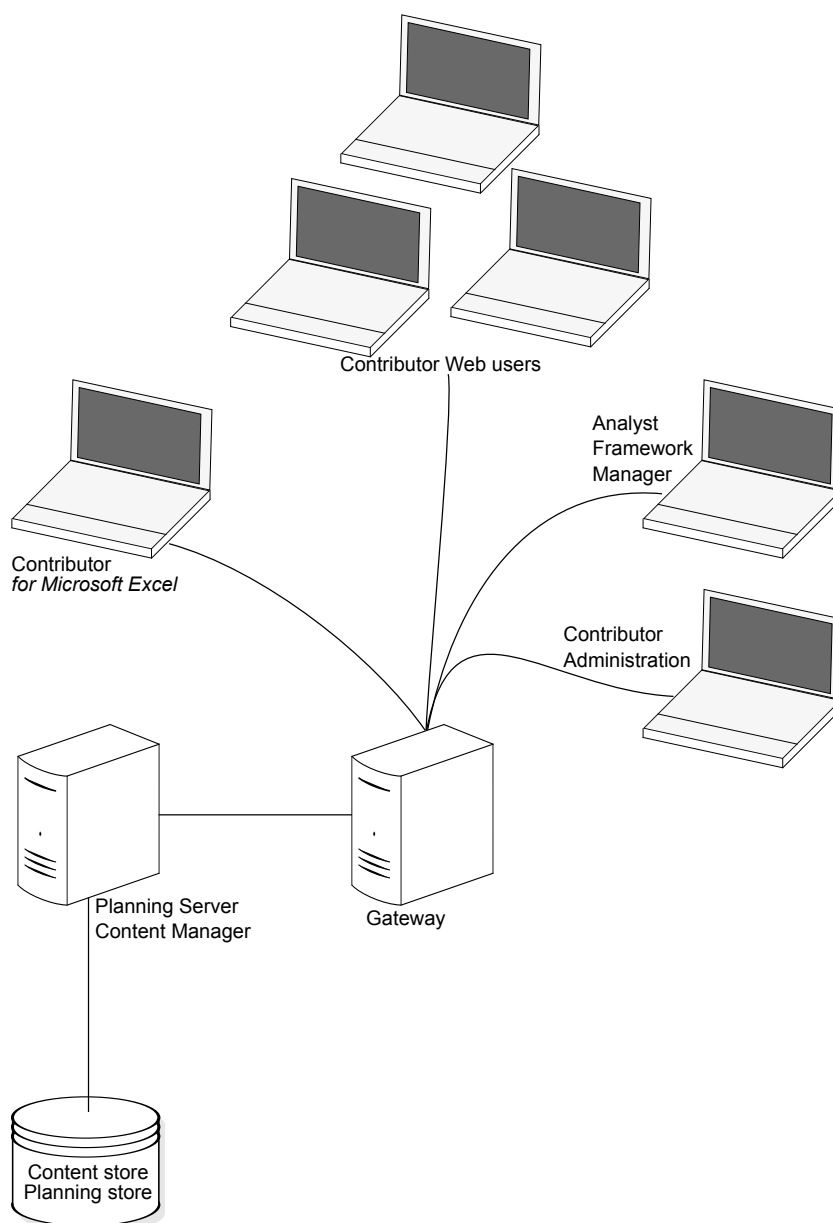
- Analyst

- Analyst *for Microsoft Excel*
- IBM Cognos Planning Manager
- Contributor Administration
- Contributor Web client
- Contributor *for Microsoft Excel*

A limited number of Analyst and Contributor Administration clients are usually installed in an environment, because most users will use either the Contributor Web or Contributor *for Microsoft Excel* clients.

Each client connects to the Planning Servers through the gateway.

The following diagram displays a sample installation of the Analyst, Contributor Administration, Contributor Web client, and Contributor *for Microsoft Excel* clients.



Installing Framework Manager

You can install Framework Manager either on a computer containing other IBM Cognos 8 Planning components, or on a computer that is separate from these other components.

To publish Framework Manager models, you must configure Framework Manager to communicate with a dispatcher, either directly or through a dedicated gateway.

We recommend that Framework Manager connect to a Planning Server dispatcher using the internal dispatcher URI. An alternative is to connect to an additional, dedicated gateway that is configured to connect to the dispatcher using the internal dispatcher URI. You must configure appropriate security for this gateway. This method is useful when the modeling tool is outside a network firewall.

Do not change your main gateway to use the internal dispatcher URI. Doing so reduces the security of IBM Cognos 8.

To ensure that Framework Manager can communicate with IBM Cognos 8 Planning components, configure cryptographic properties and the following environment properties on the computer where Framework Manager is installed:

- ☐ Gateway URI
- ☐ Dispatcher URI for external applications

For more information, see ["Install Framework Manager" \(p. 111\)](#).

Web Servers Other Than Microsoft IIS

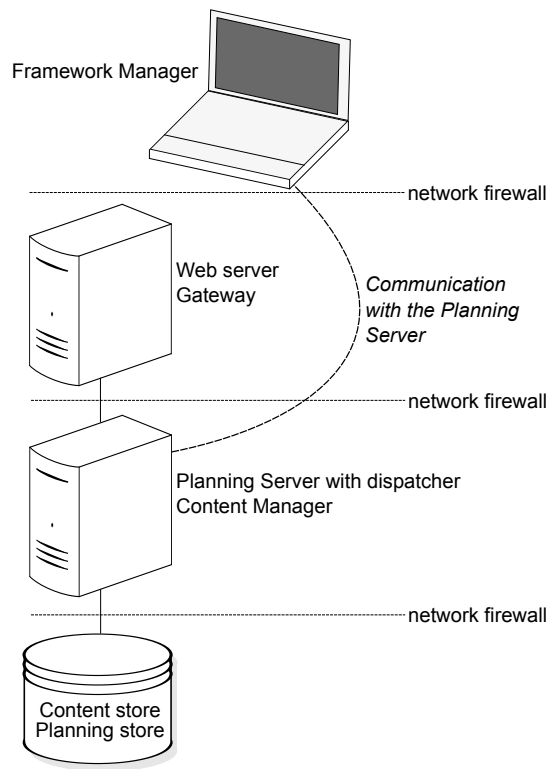
For Web servers other than Microsoft Internet Information Services (IIS), no functional difference exists between the connection alternatives for Framework Manager and the Planning Server dispatcher. For either connection, Framework Manager uses the BI Bus SOAP API. If you connect through the gateway, and you have medium-sized and large models (approaching 1 MB in size), the models are broken into smaller pieces (chunked) for transmission.

If you use a Web server other than Microsoft IIS, we recommend that you configure Framework Manager to communicate through your Web server gateway. This eliminates the need to set up additional communications channels if you use firewalls to separate Framework Manager, your Web server, and your Planning Server.

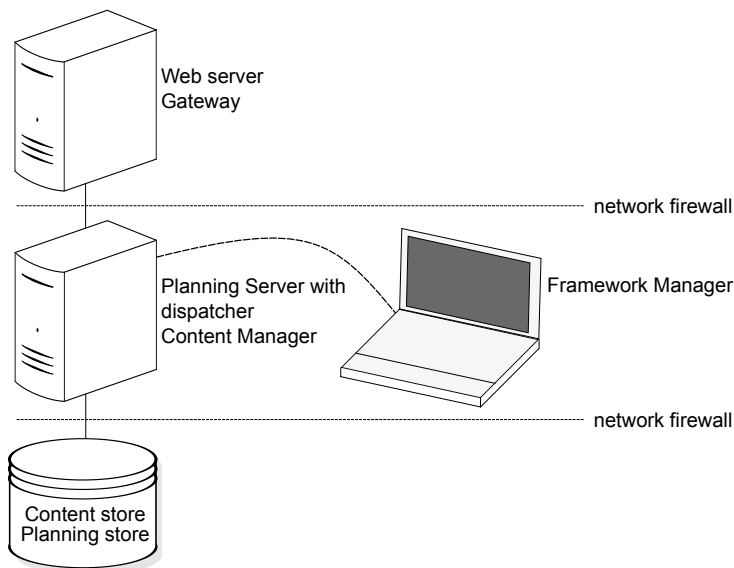
Network Firewall Considerations

When Framework Manager is outside a network firewall that protects the Planning Server computer, communication issues with the dispatcher can occur. For security reasons, the default IBM Cognos 8 configuration prevents the dispatcher from accepting requests from Framework Manager when it is outside the network firewall.

By default, Framework Manager is configured to send requests directly to the dispatcher.



To avoid communication issues when communicating directly with the dispatcher, install Framework Manager in the same architectural tier as the Planning Server.



Alternatively, you can install an additional gateway that is dedicated for communication with Framework Manager. You then configure Framework Manager and its gateway such that the dispatcher accepts requests from Framework Manager. In addition to the environment properties that must be configured for Framework Manager, you must configure the Dispatcher URIs for gateway property on the dedicated gateway computer.

Installing IBM Cognos 8 Planning with IBM Cognos 8 Business Intelligence

You can install IBM Cognos 8 Planning in an environment that includes other IBM Cognos products. The installation wizard for IBM Cognos 8 Planning will recognize compatible directories and show a warning when conflicts occur.

If you plan to install IBM Cognos 8 Planning and IBM Cognos 8 Business Intelligence in the same environment then you must ensure that the following conditions are met:

- IBM Cognos 8 Planning and IBM Cognos 8 Business Intelligence must be the same version. For example, if you already have IBM Cognos 8 Business Intelligence version 8.4 installed, then you can only install version 8.4 of IBM Cognos 8 Planning.
- Only one instance of a Planning Server or a Planning Administration tool is permitted per machine.
- Only one instance of each IBM Cognos 8 product can be installed per machine. The IBM Cognos Planning instance and the IBM Cognos BI instance must be installed in the same location.
- A machine can only belong to one environment.

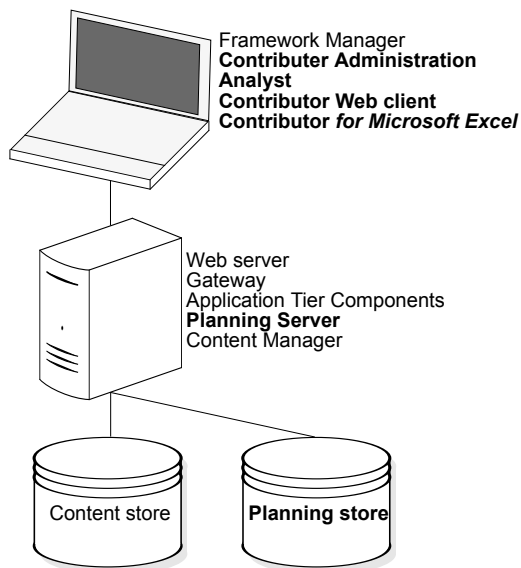
Note: Before you integrate IBM Cognos 8 Planning with IBM Cognos 8 Business Intelligence, we recommend that you consult with your Cognos Software Services representative.

You can use IBM Cognos 8 Planning published data as the basis for IBM Cognos 8 Business Intelligence reports. Report Studio and Analysis Studio users can access unpublished (real-time) and published Contributor data for analysis and reporting. You can also import data from IBM Cognos 8 data sources into Contributor applications and Analyst models. For more information, see the Contributor *Administration Guide*.

If you have an existing IBM Cognos 8 Business Intelligence environment, you can install IBM Cognos 8 Planning into that environment and use your existing IBM Cognos 8 Business Intelligence content store. If the content store is on a database platform not supported by IBM Cognos 8 Planning, you can still use the IBM Cognos 8 Business Intelligence content store, but you must use a separate planning store on a supported database.

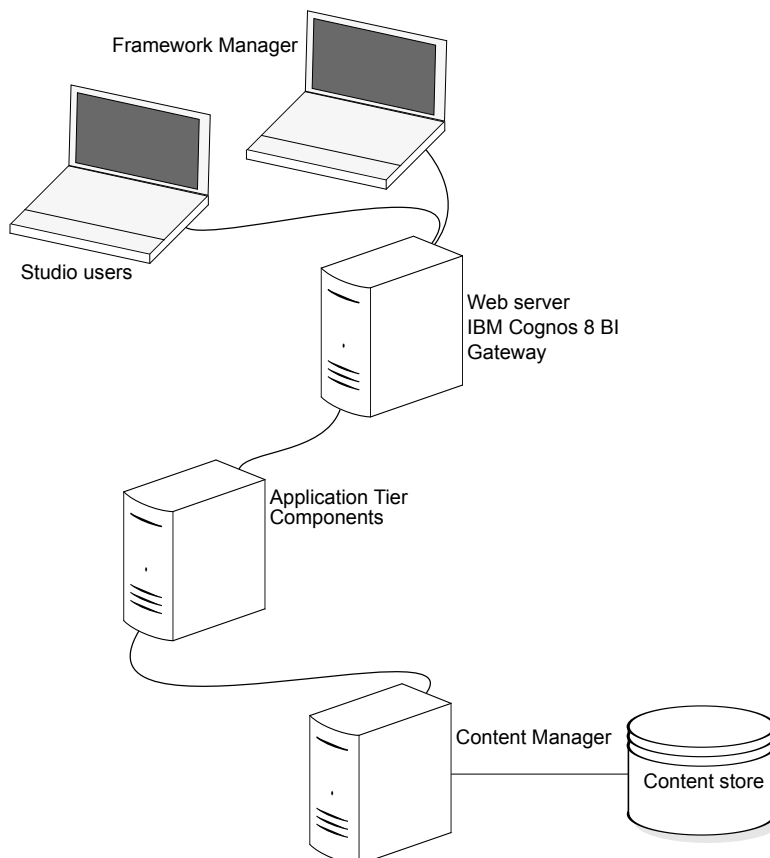
If you installed IBM Cognos 8 Business Intelligence on a single server for a demonstration or proof of concept environment, you can install the IBM Cognos 8 Planning server and clients into that environment. You can install the Planning Server component to the same location as your IBM Cognos 8 Business Intelligence Application Tier Components. You can install the clients to the same location or to another location on the same computer.

In the following diagram, the server components are installed on one computer and the clients are installed on another computer. Also, the planning store has been added as a separate database. The IBM Cognos 8 Planning components are indicated in bold text.



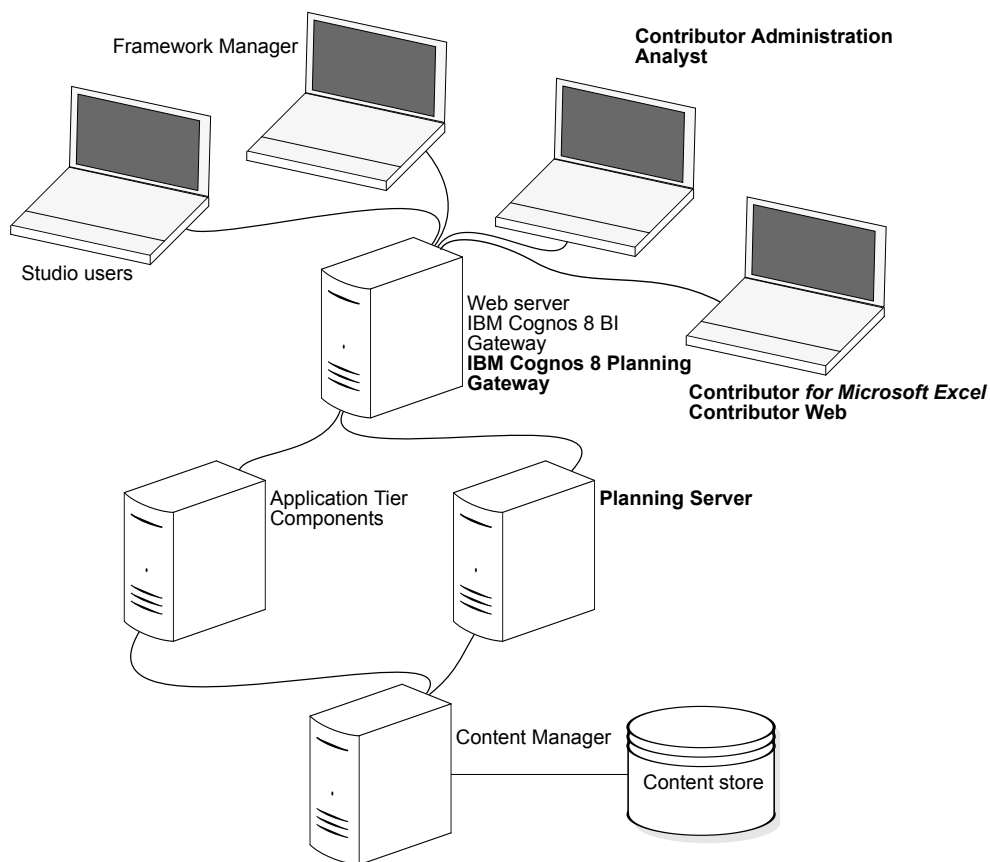
If you installed IBM Cognos 8 Business Intelligence in a distributed environment and separated the gateway, Application Tier Components, and Content Manager, you can install IBM Cognos 8 Planning into that distributed environment. In this case you can install the IBM Cognos 8 Planning gateway to the same location as your Cognos 8 Business Intelligence gateway, and you can use your existing Content Manager. To enhance performance, you may want to install the Planning Server to a separate computer.

For example, you may have an IBM Cognos 8 Business Intelligence environment that looks like this:



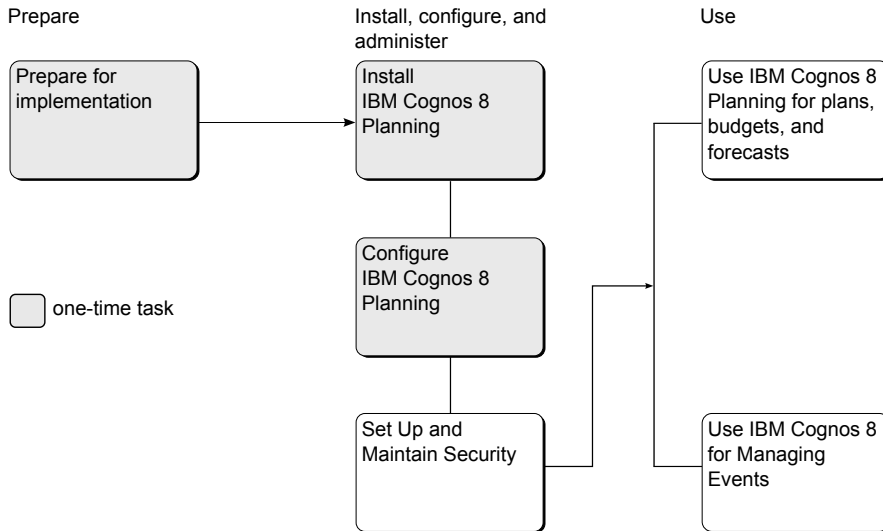
You can install the IBM Cognos 8 Planning gateway component into the same location where you installed the IBM Cognos 8 Business Intelligence gateway. Because IBM Cognos 8 Planning uses the same Content Manager as IBM Cognos 8 Business Intelligence, you do not need to reinstall Content Manager.

Your IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning environment could look like this:



Chapter 3: Workflow for IBM Cognos 8 Planning

The tasks that you must perform to install IBM Cognos 8 Planning are:



- ❑ prepare for implementation (p. 37)
This task is typically carried out by a team assembled and led by the business intelligence solutions architect.
- ❑ install (p. 37) and configure (p. 38) IBM Cognos 8 Planning
Technical personnel install and configure IBM Cognos 8 Planning, typically under the direction of a solutions architect.
- ❑ administer IBM Cognos 8
Administrators establish security and perform ongoing administration tasks using IBM Cognos Connection (p. 40).
- ❑ create and publish plans, budgets, and forecasts
Administrators create and publish plans to which Contributor users add their data. For more information, see the Contributor *Administration Guide*.
- ❑ manage events
An event is any situation that can affect the success of your business. Event Studio lets you ensure that the appropriate personnel are made aware of events.

Prepare for Implementation

Implementing IBM Cognos 8 Planning means installing and configuring it to integrate effectively with your existing infrastructure.

To ensure that IBM Cognos 8 Planning is implemented effectively, carefully outline your implementation beforehand using an implementation checklist. For more information, see the *Architecture and Deployment Guide*.

Install IBM Cognos 8 Planning

Installing IBM Cognos 8 Planning is typically done by Information Technology personnel under the direction of a solutions architect.

When you install IBM Cognos 8 Planning using the **Installation** wizard, you specify where to install each of these components:

- Planning Gateway
- Planning Servers
- Content Manager

You can install the components on one computer, or distribute them across a network. Before installing IBM Cognos 8 Planning, choose the appropriate installation and configuration option ([p. 21](#)).

You must also install the administration applications, including Analyst and Contributor Administration, and Framework Manager. The studio interfaces, such as Event Studio, are HTML- and JavaScript-based and do not require installation.

Client applications, such as the Contributor client and Contributor *for Microsoft Excel*, must also be installed on user computers.

Unattended Installation

If you plan to install an identical IBM Cognos 8 Planning configuration across several computers on a network, or to install multiple configurations, you can set up and run an unattended installation. This is a noninteractive method of installing and configuring IBM Cognos 8 Planning in which all the tasks run automatically, without user intervention. You can run the unattended installation as part of a script, or from the command line.

An unattended installation is useful if you must install IBM Cognos 8 Planning at different geographic locations, some of which have no technical personnel to perform the installation. You can also use an unattended installation if you plan to install multiple Planning Servers in your environment.

For more information about unattended installations, see "[Setting Up an Unattended Installation and Configuration](#)" ([p. 205](#)).

Configure IBM Cognos 8

Use IBM Cognos Configuration to set up your IBM Cognos 8 Planning environment. Some of the things that you can configure are

- port numbers

You can change the default port numbers used by IBM Cognos 8 Planning components.

- gateway address

You can change the default gateway address from <http://localhost/cognos8>.

- security

You can run IBM Cognos 8 with or without security. By default, the only security that is enabled is IBM Cognos Application Firewall. For IBM Cognos 8 Planning, you must apply security. IBM Cognos 8 Planning can use your existing security provider. For more information, see "[Configuring IBM Cognos 8 Components to Use an Authentication Provider](#)" ([p. 147](#)).

- data access

You must specify database connection information for the IBM Cognos 8 content store and the planning store.

- logging

You can specify the destination log for messages generated by some IBM Cognos 8 server components, such as the gateway, Content Manager, and the IBM Cognos 8 Dispatcher service. The default location for client log files is C:\Windows\Temp.

Following initial configuration, if a property changes or components are added, you can use IBM Cognos Configuration to change your settings.

Monitor Configuration Changes

Each time that you save a configuration after making changes, date-stamped versions of the following configuration files are automatically saved in the *c8_location/configuration* directory:

- cogstartup.xml

This file records configuration settings. An example file name is cogstartup_200211231540.xml.

- coglocale.xml

This file records locale settings used for multilingual reporting. An example file name is coglocale_200211261401.xml.

If you are unable to save a configuration, or you have problems with a configuration, you can revert to a previous configuration file.

You can use the configuration files to review your configuration history. Before calling Cognos Software Services for help, print a history of the configuration changes made in IBM Cognos 8.

Configure Security

IBM Cognos 8 integrates with an existing security infrastructure to provide user authentication. IBM Cognos 8 can secure content by using the user and group definitions from your security system, without any changes required.

A IBM Cognos namespace is included in case you want to define additional groups for securing content. These groups can simplify security administration by including users and groups from one or more authentication providers.

IBM Cognos 8 includes IBM Cognos Application Firewall, which is installed with the dispatcher to validate and filter incoming and outgoing traffic at the dispatcher layer. By default, IBM Cognos Application Firewall is enabled.

IBM Cognos 8 provides an authorization facility for assigning permissions to users defined in the authentication provider. It also provides a standard certificate authority (CA) for setting up encryption. Enhanced capabilities are available separately.

If you intend to set up security for IBM Cognos 8, it should be the first thing that you do after installation. For more information, see "[Configuring IBM Cognos 8 Components to Use an](#)

[Authentication Provider" \(p. 147\)](#). For information about setting up and maintaining security, see the *Administration and Security Guide*.

Administer IBM Cognos 8

After IBM Cognos 8 is installed and configured, you can use IBM Cognos Connection or your portal to

- set up folders
- make plans available to business users
- monitor and administer servers
- back up data
- maintain security

For information about using IBM Cognos Connection, see the IBM Cognos Connection *User Guide*. For information about administration, including setting up sample report projects and models, see the *Administration and Security Guide*.

Chapter 4: Setting Up Your Environment

You must set up resources in your environment for the IBM Cognos 8 components to operate. For example, you must create a database for the content store and the planning store and you must configure your Web server.

You must ensure that a Web browser and a Web server are set up to provide access to IBM Cognos components. If you use a router, you must configure it to support IBM Cognos features.

Use the following checklist to guide you through the setup process:

- ☐ [Review the Readme.](#)
- ☐ [Review the supported environments.](#)
- ☐ [Verify system requirements.](#)
- ☐ [Set up database connectivity for the content store.](#)
- ☐ [Set up database connectivity for the planning store.](#)
- ☐ [Create the database for the content store and planning store.](#)
- ☐ [Set up the database client for the content store and planning store.](#)
- ☐ [Configure Web browsers.](#)
- ☐ [Configure the router to test whether a dispatcher is available](#), if required.
- ☐ [Set up the data source environment for Framework Manager](#), if required.
- ☐ [Set up the database client for Framework Manager](#), if required.

Recommendation - Review the Readme Before You Install

Before you install your IBM Cognos product, it is important to be aware of all issues that may affect your installation strategy.

There may be late-breaking issues that were not known when this installation guide was created.

We recommend that you review the Readme before you install your product. The Readme contains late-breaking information about known issues as well as documentation updates and deprecation notices. The Readme is available from the first page of the installation wizard or from the product CD.

Review Supported Environments

To ensure your product works properly, apply all required operating system patches and use only the versions of other software that are supported for an IBM Cognos product.

To review an up-to-date list of environments supported by IBM Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers

- Visit the Cognos Software Services Web site (<http://support.cognos.com>).

Verify System Requirements

Use the following table to check the minimum hardware and software requirements to install and run IBM Cognos 8 components on one computer. Additional resources may be required for distributed or production environments.

Requirement	Specification
Operating system	Windows
RAM	Minimum: 2 GB per processor
RAM	Minimum for Planning Client: 512 MB
Disk space	A minimum of 2.5 GB of free space is required to install the software and 1 GB of free space on the drive that contains the temporary directory used by IBM Cognos components.
Web server	A Web server must be installed and started.
Database	<p>You must have one of the following databases available to store IBM Cognos data:</p> <ul style="list-style-type: none">• Oracle• DB2• Microsoft SQL Server <p>TCP/IP connectivity to Microsoft SQL Server</p> <ul style="list-style-type: none">• Sybase <p>Sybase can only be used for the content store. You cannot use Sybase for the planning store.</p>

Requirement	Specification
Web browser	<p>For all Web browsers, the following are enabled:</p> <ul style="list-style-type: none"> • cookies • JavaScript <p>For Microsoft Internet Explorer only, the following are enabled:</p> <ul style="list-style-type: none"> • Run ActiveX controls and plug-ins • Script ActiveX controls marked safe for scripting • Active scripting • Allow META REFRESH
Other	<p>On Windows, Microsoft Data Access Component (MDAC) for use with product samples</p> <p>If you want to email reports, the ability to use a mail server</p>
SAP BW	<p>The following SAP Front-End components installed on each IBM Cognos 8 server computer:</p> <ul style="list-style-type: none"> • SAP GUI 6.40 • BW Add-ons

Set Up Database Connectivity for the Content Store Database

Database client software must be installed and configured on each computer where you install Content Manager.

To set up database connectivity for the content store database:

- Install the appropriate JDBC driver for your Content Manager database, as follows:

Database	JDBC Driver
DB2	JDBC driver that requires DB2 client installation
Oracle	<p>JDBC thin driver, ojdbc14.jar</p> <p>For Oracle 11g, ojdbc5.jar</p> <p>If the directory contains the classes12.jar file, you must delete it before installing the ojdbc14.jar or ojdbc5.jar file.</p>

Database	JDBC Driver
Microsoft SQL Server	Included with IBM Cognos components. No other software is required. IBM Cognos 8 requires TCP/IP connectivity with Microsoft SQL Server.
Sybase	JDBC driver, jconn2.jar

Set Up Database Connectivity for the Planning Store Database

For IBM Cognos 8 Planning, all Planning Server computers must be able to access the planning store using the object linking and embedding database (OLEDB) API.

You must install the appropriate OLE DB database driver on each computer where you install Planning Server components to set up database connectivity for the planning store database.

Note: If you configure MS SQL Server Windows Authentication for the planning store databases, you must take into account that the planning data service inherits its security from the dispatcher.

Create the Content Store and Planning Store

The content store is a database that Content Manager uses to store global configuration data, global settings (such as the language and currency formats shown in the user interface), connections to data sources, and product-specific content. The planning store contains macros, links, access rights, system settings, and application linking information for your planning applications.

You can use the same database for both the content store and the planning store. Alternatively, you can use separate databases in the same database instance, or in different database instances.

You can use any of the following supported databases for the content store:

- Microsoft SQL Server
- Oracle
- DB2
- Sybase Adaptive Server Enterprise (ASE)

The planning store can be on any of the following supported databases:

- Microsoft SQL Server
- Oracle
- DB2

If you use Sybase for the content store, you must use another supported database for the planning store.

A Microsoft SQL Server or Oracle database can use UTF-8 or UTF-16 encoding. A DB2 or Sybase database must use UTF-8 encoding. The database you use for the content store must use the TCP/IP protocol.

Note: IBM Cognos 8 uses a single sort order that specifies the rules used by the database to interpret, collect, compare, and present character data. For example, a sort order defines whether the letter A is less than, equal to, or greater than the letter B; whether the collation is case sensitive; and whether the collation is accent sensitive. For more information about collation and collation sequences, see the database vendor documentation.

We recommend that your database administrator back up IBM Cognos 8 databases regularly because they contain the IBM Cognos data. To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

Steps for Microsoft SQL Server 2005

1. Ensure that your installation of Microsoft SQL Server is configured as follows:

- UTF-8 or UTF-16 encoding is used

For more information about character sets, encoding, and collation, see the Microsoft SQL documentation.

- the collation sequence is case-insensitive

In a Custom installation, you choose a collation, which includes character sets and sort order, during the SQL Server setup. In a Typical installation, the installation uses the locale identified by the installation program for the collation. This setting cannot be changed later.

- the TCP/IP protocol is enabled

This protocol is required by IBM Cognos 8 to access data.

2. Open Microsoft SQL Server Management Studio and connect to the database server using SQL server authentication.

If you connect using Windows authentication, the database that you create will also use Windows authentication. IBM Cognos 8 is configured by default to use a database with SQL server authentication.

3. Create the database.

If you connected to the database server using Windows authentication, you must configure the database connection using a database type of **SQL Server database (Windows Authentication)** in IBM Cognos Configuration.

4. Create the user account that will be used to access the database:

- Under **Security**, right click **Logins** and select **New Login**.
- Specify a Login name.
- Select **SQL Server authentication** and specify the **Password**.
- Clear **Enforce password policy**.

This clears all three check boxes.

- Click **OK**.

Tip: If you want to host more than one content store on your Microsoft SQL Server instance and you will use both at the same time, use a different user account for each content store to ensure that each IBM Cognos 8 instance is fully isolated from the others.

5. Create a schema:

- Under **Databases**, expand the database (*new_database*) that you created in step 3.
- Under *new_database*, expand **Security**.
- Right-click **Schemas** and select **New Schema**.
- Specify the **Schema name** and click **OK**.

6. Configure the database user:

- Under **Databases**, *new_database*, **Security**, right click **Users** and select **New User**.
- Specify the **User name**.
- For **Login name**, browse and select the login that you created in step 4.
- For **Default schema**, browse and select the schema that you created in step 5.
- In the **Owned Schemas** list, select the same schema as **Default schema**.
- In the **Role Members** list, select **db_datareader**, **db_datawriter**, and **db_ddladmin**.
- Click **OK**.

7. Repeat steps 4 to 6 for each new user account.

Steps for Oracle

1. Ensure that the parameter for the database instance compatibility level of the content store database is set to 9.0.1 or higher.

For information about changing an instance configuration parameter, see the Oracle documentation.

2. Determine if the database is Unicode.

Tip: One method is to type the following select statement:

```
select * from NLS_DATABASE_PARAMETERS
```

The result set returns NLS_CHARACTERSET as UTF-8 or UTF-16, or AL32UTF8 or AL16UTF16, or not Unicode.

If the result set returns an NLS_CHARACTERSET that is not Unicode, create a new database and specify AL32UTF8 or UTF-8 for the database character set parameters.

3. Determine which user account will be used to access the database.

Tip: If you want to host more than one content store on your Oracle instance and you will use both at the same time, use a different user account for each content store to ensure that each IBM Cognos 8 instance is fully isolated from the others.

4. Ensure that the user account that accesses the database has permission to do the following:
 - connect to the database
 - create, alter, and drop tables, triggers, views, procedures, and sequences
 - insert, update, and delete data in the database tables

Steps for DB2

1. Set the following environment variables for DB2.

Environment variable	Description
DB2DIR	The top level directory that contains the database client software or the entire database installation.
DB2INSTANCE	The default database server connection.
DB2CODEPAGE	Setting this optional environment variable to a value of 1208 provides support for multilingual databases. For information about whether to use this environment variable, see the DB2 documentation.

2. Create a database and ensure that you select **UTF-8** as the code set value.

To check if your database has the correct code set, using the command line interface, type the following at the command prompt:

db2 get database configuration for *database_name*

The code set value should be UTF-8 and the code page value should be 1208.

3. Ensure that you set the following configuration parameters for the database.

Parameter	Setting
Application heap size (applheapsz)	1024k
Lock timeout (locktimeout)	240 seconds Do not set this to an infinite timeout value.

4. Create a buffer pool with a page size of 32 k, and a second one with a page size of 4 k.
 5. Create a system temporary tablespace using the 32 k buffer pool you created in the previous step.
 6. Create a user temporary tablespace using the 4 k buffer pool you created in step 4.
Global temporary tables will be created in the user temporary tablespace.
 7. Create a regular user tablespace using the 4 k buffer pool you created in step 4.
If you are also creating a logging database, create an additional regular user tablespace with a page size of 8 k.
 8. Grant the following database privileges for the user account IBM Cognos 8 will use to access the database:
 - connect to database
 - create tables
 - create schemas implicitly
- Tip:** If you want to host more than one content store on your DB2 instance and you will use both at the same time, use a different user account for each content store to ensure that each IBM Cognos 8 instance is fully isolated from the other.
9. Ensure that the user account has use privileges for the user temporary tablespace and other appropriate tablespaces associated with the database.
On Windows XP, ensure that the user account has grant privileges for the user temporary tablespace.
 10. Create a schema for the user account IBM Cognos 8 will use to access the database, and ensure the user has create, drop, and alter permissions for the schema.

Steps for Sybase Adaptive Server Enterprise

1. On the Sybase server, create a server instance with an 8K server page size.
For instructions, see the Sybase documentation.
2. If required, install jConnect 5.5.
This tool sets up the communication between the JDBC driver and the Sybase Adaptive Server instance.
For instructions, see the Sybase documentation.
If your version of Sybase does not include JConnect 5.5, you must download the installer from Sybase's Web site.
3. Add the UTF-8 character set to the server instance.
4. If required, make UTF-8 the default character set on the server.
5. Create a database device.

Tip: Set `log_segment` to a minimum of 10 MB.

6. Set the new database device as the default.

Information about the new database will be stored in the new database device. Keep a backup of the database device for recovery purposes.

7. Create the database.
8. Determine which user account will be used to access the database.

Tip: If you want to host more than one content store on your Sybase instance and you will use them at the same time, use a different user account for each content store to ensure that each IBM Cognos 8 instance is fully isolated from the others.

9. Grant create and drop table privileges on the database to the user account.

Ensure that the user account has the following privileges for the database: create default, create procedure, create rule, create table, and create view.

10. For the database, set the **Select into** property to True and restart the server.

Set Up the Database Client

For the planning store, you must ensure that the appropriate OLE DB drivers are installed on each computer where Content Manager or a Planning Server is installed.

For the content store, you must ensure that the appropriate JDBC drivers are installed every computer where Content Manager or Framework Manager is installed, as shown in the following table.

Database	Additional Steps
DB2	Set up the database client software and the JDBC 2.0 driver.
Oracle	Set up the JDBC driver.
Sybase	Set up the JDBC driver.
Microsoft SQL Server	No additional steps are required. The JSQConnect.jar is installed to the appropriate location by default.

The following steps are for configuring the database client for the content store.

Steps for DB2

1. Install the DB2 client software on the appropriate computers.
2. If the content store is on a different computer from Content Manager, configure a database alias to the content store by running the DB2 Client Configuration Assistant.

If the content store database and Content Manager are on the same computer, the content store name automatically becomes the alias.

When you configure the Content Manager computers, ensure that they are all configured to use the same content store.

3. On Windows, stop the DB2 services and the HTML Search Server.
4. To copy the JDBC2 driver, copy the *DB2_installation/sql/lib/java/db2java.zip* file to the *c8_location/webapps/p2pd/WEB-INF/lib* directory.
5. Rename the db2java.zip file to db2java.jar.
6. On Windows, restart the DB2 services and the HTML Search Server.
7. Repeat this entire procedure on the IBM Cognos 8 computers where the software must be installed.

Steps for Oracle

1. On the computer where the Oracle client is installed, go to the *ORACLE_HOME/jdbc/lib* directory.
2. Copy the ojdbc14.jar file (or, for Oracle 11g, the ojdbc5.jar file) to the *c8_location/webapps/p2pd/WEB-INF/lib* directory on computers where Content Manager is installed.

If the directory contains the classes12.jar file, delete it before installing the ojdbc14.jar or ojdbc5.jar file.

This file includes the driver required by the content store.

You can tune the database to take advantage of DB2 features. For more information, see the *Architecture and Deployment Guide*.

Steps for Sybase

1. On the computer where Sybase is installed, go to the *Sybase_location/jConnect-5_5/classes* directory.
2. Copy the jconn2.jar file to the *c8_location/webapps/p2pd/WEB-INF/lib* directory on every computer where Content Manager is installed.

Configure Web Browsers

IBM Cognos 8 uses the default Microsoft Internet Explorer browser configuration. However, you must ensure that settings are enabled for cookies and Java scripts.

The following table shows the settings that must be enabled.

Browser	Setting	IBM Cognos component
Internet Explorer (settings for studios and portals)	Allow Cookies	IBM Cognos Connection
	Active Scripting	IBM Cognos Administration
	Allow META REFRESH	IBM Cognos Viewer
		Event Studio

IBM Cognos 8 uses the following cookies to store user information.

Cookie	Type	Purpose
AS_TICKET	Session temporary	Created if IBM Cognos 8 is configured to use an IBM Cognos Series 7 namespace
caf	Session temporary	Contains security state information
Cam_passport	Session temporary	Stores a reference to a user session stored on the Content Manager server
cc_session	Session temporary	Holds session information that is specific to IBM Cognos Connection
cc_state	Session temporary	Holds information during edit operations, such as cut, copy, and paste
CRN	Session temporary	Contains the content and product locale information, and is set for all IBM Cognos users
CRN_RS	Persistent	Stores the choice that the user makes for "view members folder" in Report Studio
PAT_CURRENT_FOLDER	Persistent	Stores the current folder path if local file access is used, and is updated after the Open or Save dialog box is used

Cookie	Type	Purpose
pp_session	Session temporary	Stores session information that is specific to PowerPlay Studio
qs	Persistent	Stores the settings that the user makes for user interface elements such as menus and tool-bars
usersessionid	Session temporary	Contains a unique user session identifier, valid for the duration of the browser session.

After upgrading or installing new software, restart the Web browser and advise users to clear their browser cache.

Configure the Router to Test Dispatcher Availability

If you use a router to distribute requests to IBM Cognos 8 dispatchers, and the router can test the availability of a server using a test URL, you can configure the router to test the availability of an IBM Cognos 8 dispatcher.

To test the availability of a dispatcher, do the following:

- Configure the router to use a URL with the path /p2pd/servlet/ping.

If the dispatcher is not ready, the following response is returned:

503 Service Unavailable

If the dispatcher is ready, the following response is returned:

200 OK

Set Up the Data Source or Import Source Environment

Framework Manager is the IBM Cognos 8 modeling tool that can be used with IBM Cognos 8 Planning to create and manage metadata from other data sources to be used in plans. Metadata is derived from data sources in multi-platform or multilingual environments. Keep this in mind when you set up the data source environment for Framework Manager or the import source environment for Analyst.

If you upgraded from an older version of Framework Manager, you are not required to set up anything in the data source environment. You must set up the data source environment only if you installed Framework Manager in a different location from the older version.

Ensure that you install the appropriate language packs to support the character sets and currency symbols you use. For information about installing language packs, see the IBM Cognos Supplementary Languages *Installation and Configuration Guide*.

If users operating in different languages will be connecting to a Microsoft Analysis Services (MSAS) data source, you must create a separate IBM Cognos 8 instance for each language.

Steps

1. Set the environment variable for multilingual support:

- For Oracle, set the NLS_LANG (National Language Support) environment variable on each computer where Framework Manager and the IBM Cognos 8 Planning server are installed by typing the following command:

NLS_LANG = language_territory.character_set

Examples are:

NLS_LANG = AMERICAN_AMERICA.UTF8

NLS_LANG = JAPANESE_JAPAN.UTF8

The value of the variable determines the locale-dependent behavior of IBM Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

- For DB2, set the DB2CODEPAGE environment variable to a value of 1252.

For more information about whether to use this optional environment variable, see the DB2 documentation.

No settings are required for SAP BW. SAP support only a single code page on non-Unicode SAP BW systems.

2. For Oracle, add \$ORACLE_HOME/lib to your LD_LIBRARY_PATH.

When you set the load library paths, ensure that the 32-bit Oracle libraries are in the library search path, which is usually the \$ORACLE_HOME/lib directory or the \$ORACLE_HOME/lib32 directory if you installed a 64-bit Oracle client.

3. For Oracle, copy the ojdbc14.jar file from ORACLE_HOME/jdbc/lib to the *c8_location/webapps/p2pd/WEB-INF/lib* directory.
4. For SAP BW, configure the authorization objects so that the modeling tool can retrieve metadata.

For more information about SAP BW authorization objects, see ["Set Access Permissions for Modeling and Reporting Access" \(p. 186\)](#).

After you complete these tasks, you must configure the IBM Cognos 8 Planning components to work in your environment.

Chapter 5: Upgrading to IBM Cognos 8 Planning

New versions of IBM Cognos Planning provide enhancements of product features and functionality, performance and scalability, and usability. Because of these improvements, upgrading may not be simple, and should be considered a process that you perform in stages.

Note: IBM Cognos 8 Planning version 8.4 is a major upgrade. For this reason, we recommend that you create a new environment for Planning version 8.4, starting with a clean content store.

You should treat upgrading as an IT project that requires careful planning, adequate time, and resources.

When you upgrade, you perform two distinct activities:

1. Install the new version of the product.
2. Move applications to the new version of the product.

Install the New Version of the Product

You can install the new version of the product in the same location as the existing version after you uninstall, or you can install into a new location.

You can configure your new environment to use the content store and planning store you used for your previous environment.

We recommend that you first install into a new location, such as a test environment. This allows you to test your applications in both the old and new environment to ensure that they work as expected when you upgrade. You can compare the appearance and functionality of the reports in both environments to ensure equivalency.

Also, ensure that you back up your Planning Administration Domain and any other applications before you upgrade.

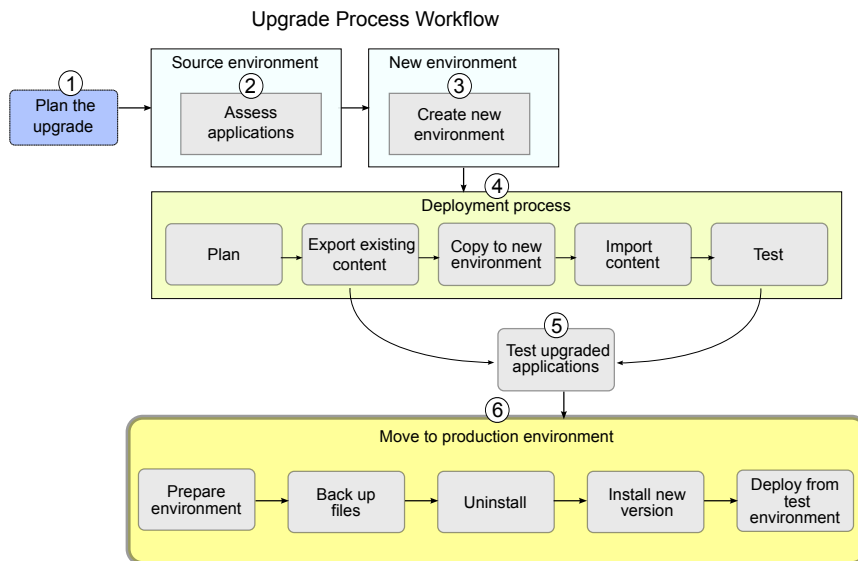
Move Content to the New Environment

As part of the upgrade process, ensure that your applications work as expected in the new version. Sometimes, changes may introduce unexpected results. It is important to test your applications before you move them to the production environment.

In IBM Cognos 8 Planning, when you move content from one environment to another, you do a deployment.

Upgrade Process

The following diagram shows the approach that we recommend when you upgrade from version 8.2 and above. The diagram shows the stages in the upgrade process. Before you start, you plan the upgrade, assess the applications that you want to upgrade, and create a test environment. You should iteratively deploy and test content in both the source and target environments before you move successfully upgraded applications to a production environment.



In some upgrade situations, other tasks may be required. For example, the process of upgrading from versions 7.2, 7.3, and 8.1 is different. For more information about this process, see ["Upgrading From Versions 7.2, 7.3, or 8.1" \(p. 68\)](#).

Different groups are commonly involved in each of these activities. As part of the project, you should assess both your current IT environment and your existing applications separately, to ensure that the infrastructure can support your business objectives.

See the following topics for information about upgrading:

- ☐ [Upgrading IBM Cognos Business Intelligence.](#)
- ☐ [Choosing the Upgrade Tool.](#)
- ☐ [Planning the Upgrade.](#)
- ☐ [Upgrading the Planning Administration Domains.](#)
- ☐ [Upgrading Planning Applications.](#)
- ☐ [Upgrade Analyst Security and Library Files.](#)

Upgrading IBM Cognos 8 Business Intelligence

To use IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning products together, both products must be the same version. For example, if you have BI installed with your existing version of Planning, you must upgrade BI to version 8.4 before you can use Planning version 8.4 and IBM Cognos 8 BI together.

For more information about upgrading IBM Cognos 8 BI, see the *IBM Cognos 8 Business Intelligence Installation Guide*.

Choosing the Upgrade Tool

You can upgrade users, user classes, groups, libraries, and Contributor applications from previous IBM Cognos Planning versions. Depending on your version, you can upgrade the entire Planning Application Database or you can upgrade individual applications.

Use the following table to determine which upgrade tool you need according to the version of Planning you currently have installed.

Upgrade Tool	Current Planning Version	Description
Planning Administration Domain Wizard	7.3 8.1	Upgrades applications, administration links, and macros from the source Planning Administration Domain. The security and access rights for the Planning Administration Domain objects are remapped in the new environment.
Upgrade Application Wizard	7.2 7.3 8.1	Upgrades individual or multiple applications at once. The security of each application is updated in the new environment, but the access rights are not updated.
Deployment Wizard	8.2 or higher	Enables you to export and import complete models, macros, administration links, or Analyst libraries. You can export individual or multiple Planning Administration Domain objects.

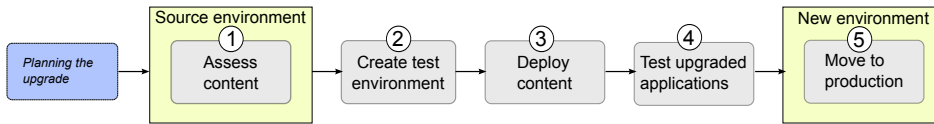
Planning the Upgrade

We recommend that you plan your upgrade so that you know what to expect at each stage of the process. In the planning stage, you can review the upgrade documentation for information about the

- expected behavior
- new features
- deprecated features
- compatibility between versions
- requirements for preparing your production environment

When you finish the review, you can then conduct a site survey to identify the infrastructure, applications, and custom configuration settings. Finally, you can test the upgrade on a subset of your data to fine tune your plans, applications, and data before committing to the full upgrade.

The following diagram shows a high level view of the phases in an upgrade project.



When planning your upgrade, ensure that you

- gather the necessary information, such as the required inputs and expected outputs for each phase
- assess the applications in your environment
- install the new software in a test environment and deploy the content to the test environment
- test the upgraded applications

Deployment and testing is usually an iterative process. Assess any differences between the source and target environments to determine actionable activities. Move to your production environment when you are satisfied that the deployed applications meet your business requirements.

We recommend that you do not change security providers, such as changing from a Cognos Series 7 namespace to Active Directory as part of the upgrade process. You should treat that as a separate project.

Ensure that you have the skills available, either internal or using external resources. Also consider the hardware that you will need before you begin.

Use the following checklist to guide you through the planning process:

- ☐ [Review the documentation.](#)
- ☐ [Assess applications in the source environment.](#)
- ☐ [Perform a trial upgrade:](#)
 - [Create the test environment.](#)
 - [Plan the deployment of content](#) from the source environment to the test environment.
 - [Create an export deployment specification.](#)
 - [Copy the deployment specification to the test environment.](#)
 - [Import the deployment specification](#) to Cognos 8 in the test environment.
 - [Test the upgraded content.](#)
- ☐ [Move to the production environment.](#)

Review the Documentation

Documentation is provided from a variety of sources to help you achieve a successful upgrade. All the documentation is available online at the Cognos Software Services Web site (<http://support.cognos.com>).

Steps

1. Read the "What's New" section in this guide ([p. 13](#)).
It contains a list of new, changed, deprecated, and removed features for this release.
2. Read the rest of the Upgrade information in this document.
3. From the Documentation link on the Cognos Software Services Web site (<http://support.cognos.com>), download and review the latest versions of the following documentation:

Document	Description
IBM Cognos 8 Planning <i>Readme</i>	Recent Planning issues that may affect an upgrade
IBM Cognos 8 <i>Readme</i>	Recent IBM Cognos 8 issues that may affect an upgrade
IBM Cognos 8 Planning <i>New Features Guide</i>	New features that may affect the behavior of existing content
Framework Manager <i>User Guide</i>	Upgrading models

Recommendation - Assess Applications in the Source Environment

Preparing to upgrade provides an opportunity to review your current Planning investment, and clean up your source environment. Inventory your Planning applications to understand the strengths, weaknesses, and areas for improvement in your environment.

For example, you may have a hundreds applications in your environment. However, it is not uncommon to find that a number of applications are not used, no longer meet the company's requirements, or do not work in the source environments.

We recommend that you conduct an audit of your applications to determine which applications you should upgrade. Assessing and reducing the number of applications is a useful exercise. Do not rely only on user feedback to determine which content is used.

An audit of your existing applications may include the following tasks:

- ☐ Do a site survey.

Assess the current production environment and identify areas that require attention during an upgrade. The site survey includes information about the infrastructure, applications, users, and configuration settings.

- ❑ Assess the software that you use in your environment.

List software, such as operating systems, Web servers, security, databases. Compare the list to the supported versions for your target upgrade version, available from the Production Information, Software Environments links at the Cognos Software Services Web site (<http://support.cognos.com>). Determine whether any components require updating.

- ❑ Complete a detailed assessment of your applications.

The usage, age, size, and complexity of your applications are important factors to consider when planning the upgrade. The total size of the applications may have an impact on the time required to complete the upgrade.

- ❑ List the following information about your configuration:

- configuration settings that you enabled using IBM Cognos Configuration

These settings are preserved through the upgrade. They are stored in two files, `cogstartup.xml` and `coglocale.xml`.

- changes to other configuration files

You must make the changes manually to other configuration files during the upgrade. If you changed other configuration files, you must assess the changes that you want to preserve in the upgraded environment. This may include `.xml`, `.txt`, and `.css` files in the configuration, templates, webapps, and webcontent directories of the installation location.

Important: Changes to `.ini` files are not supported. If you changed `.ini` files, please contact Customer Support.

- ❑ Back up all reports, models, configuration data, and files.

Once your audit is complete, you can create an upgrade plan.

Recommendation - Perform a Trial Upgrade

Pilot upgrade projects are valuable and practical exercises because they ensure that the upgrade produce the expected and required outcome. In addition, an evaluation of the pilot project ensures that the upgrade is successful. If unexpected results occur, you can determine whether the differences are enhancements for your situation or whether you should take action to mitigate the differences.

When you upgrade, applications usually work in the new environment, with little or no intervention. By running an pilot upgrade you can validate selected applications to see if the expected results are produced.

We recommend that you perform a trial upgrade several weeks before upgrading your production system. The trial upgrade identifies components that will upgrade with minimal effort, and components that may require additional actions before or after the upgrade.

Ensure skilled resources are available to perform migration work, especially for mission-critical applications. Also, test and debug all applications prior to deployment.

Create the Test Environment

Create a test environment for the new software in preparation for your trial upgrades.

Initially, the new environment does not need to be large, or be the same as your production environment. For example, if it is acceptable, you may use hardware from existing environments, such as development servers.

The environment can be scaled up and out in a phased way after the basic new environment is up and running.

Alternatively, existing environments can remain untouched. If you want the test environment to become the new production environment, configure the test system to match your production environment.

Steps

1. Ensure the infrastructure is in place.
2. Review the supported environments.
3. Install the new software in the test environment.

For more information about basic installations, see [Installing and Configuring IBM Cognos 8 Planning on One Computer](#).

After you install the software, use the deployment process to upgrade the content. For more information, see the IBM Cognos 8 Planning - Contributor *Administration Guide*.

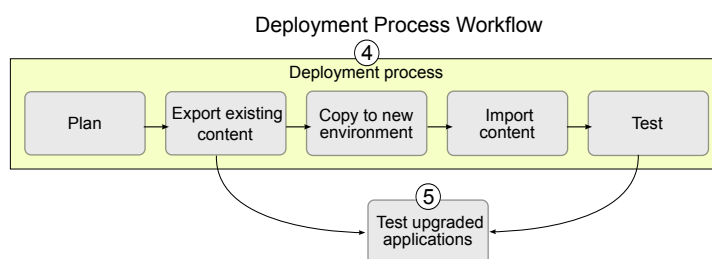
Plan Your Deployment

Deployment involves moving applications, models, macros, administration links, or Analyst libraries from one installation to another.

When you deploy, you must consider how to handle security and whether to deploy the entire content store or to deploy selected packages, folders, and directory content. Other considerations relate to the database you use for the content store, bursting reports, and ownership of entries.

For more information about planning the deployment of content to a new environment, see the Contributor *Administration Guide*.

The following diagram summarizes the deployment process.



Security

Before you deploy, you must consider access permissions and security of deployment archives.

To deploy IBM Cognos Connection entries, you must have the following permissions:

- Execute permissions for the **Administration tasks** secured feature.
- Traverse permissions for the **Administration** secured function.

We also recommend that you belong to the System Administrators group, and have read and write access to the IBM Cognos namespace, so that you can deploy the System Administrators group.

For more information about security and deployment, see the Contributor *Administration Guide*.

References to Namespaces

Some entries, such as groups, roles, distribution lists, contacts, data source signons, and some report properties, such as email recipients and report contacts, can refer to entities in namespaces, or authentication providers. When you deploy public folders and directory content, you can deploy these entries with or without the third-party references.

Deploying the Entire Content Store

Deploying the entire content store ensures that all the data is copied to a new location. For example, if you are moving Planning to another computer, you can move the entire content store from the old environment to the new environment.

When you import an entire content store, configuration data is included in the export, but excluded from the import by default. We recommend that you do not change this setting.

Create an Export Deployment Specification

After planning your deployment, the first step in moving content from the one installation to another is to export the content store or the entries that you want to keep in your new environment. To do this, use the Contributor Administration Console to create a deployment specification in your source environment.

The entries are exported to an export deployment archive in the source environment. Later, you import the archive entries into the target environment.

You can export complete models, macros, administration links, or Analyst libraries with or without the associated data from Planning - Contributor or Analyst. You deploy a model by exporting it from one environment and importing it into another.

When you export a model, the reports, events, or Framework Manager models associated with the Planning Administration Domain are not exported.

The model structure and data are exported to the deployment directory location set in IBM Cognos Configuration.

You can backup an application by exporting it, but we do not recommend this as a substitute for database backup.

The default deployment location is `c8_location\deployment`.

We recommend that you stop the IBM Cognos 8 service before you export and import.

Steps

1. From the **Tools** menu, click **Deployment** and then click one of the following:
 - **Export Model**
 - **Export Model and Data**

2. In the **Welcome to the Export Deployment Wizard** page, click **Next**.
3. Select the objects you want to export and click **Next**.

Selecting a top level object will select all the children of that object.

4. Type a new name for the export, or choose a name from existing deployments and click **Finish**.
5. Click **OK**.

Copy the Deployment Specification to the Test Environment

Transfer the deployment to a test environment, then move the export folder from the source deployment directory location to the deployment directory location for the test environment.

Later, you use the deployment archive to import entries into the target environment.

If you plan to move the deployment archive to a location on a LAN, ensure that there is enough disk space.

Import to the Test Environment

You can import a model or object to move an application into a test or production environment. Models for import must be in the deployment directory location set in IBM Cognos Configuration.

You can import macros, administration links, applications, Analyst libraries, and security rights from the source Planning Content Store that were exported during a previous deployment. You can select exported objects for import or import an entire model. If a model was exported with data, then the data will be used during the import.

You can import administration links and macros even if they reference an application that is not in the target destination. If imported with a related application, macros and administration links are automatically mapped to the target application.

Through the import process, you can change the target datastore and security for your model. The deployment wizard attempts to map security settings for users, groups, and roles. If you are using different namespaces or changing user, group, or role mappings, you may have to complete some of the mapping manually.

The security settings for the source are applied to the user, group, or role to which you map. You can map source users, groups, and roles together or individually to any single target user, group, or role. When mapping a number of users, groups, or roles, the target maintains the greatest level of security privileges. Any unmapped items are mapped to Planning Rights Administrator and do not appear individually as a user, group, or role in the target.

Application IDs and object names must be unique within the Planning Administration Domain. During the import processes, if duplicate names or IDs are found, you are warned. If you proceed with the import without changing names and IDs, then any existing applications or objects with common names or IDs will be overwritten.

To import Contributor applications, you must have at least one configured datastore and the Planning content store must be added to a job server. A datastore is not required to import Analyst libraries, macros, or administration links.

Steps

1. From the **Tools** menu, click **Deployment** and then click **Import**.
2. In the **Welcome to the Import Deployment Wizard** page, click **Next**.
3. In the **Deployment Archive Name** page, select a deployment to import and click **Next**.
4. In the **Import Object Selection** page, select the objects for import and click **Next**.
Selecting a top level object selects all the children of that object.
5. In the **Namespace Mapping** page, select the target namespace for each source namespace, and click **Next**.
6. The **User Group Role Mapping** page contains a tab for each namespace mapping. For each mapping, assign the correct target user, group, or role to each source by clicking the ellipsis (...) button.
7. On the **Select entries (Navigate)** page, in the available entries directory, click the namespace that contains the target user, group, or role.
8. From the selected entries, select the target user, group, or role and click **OK**.
9. Complete the user, group, or role mapping for each Namespace mapping. Once you have completed mapping each source user, group, or role to the target, click **Next**.
10. For each application or library with a warning next to it in the **Object Mapping** page, click the ellipsis (...) button to change the configuration settings. You can also map all target options by clicking **Map All** and adding a prefix or suffix to the object names. You can also set the job server cluster for the application.
11. On the **Configuration settings** page, type new names, IDs and locations of files, and click **OK**.
For an Oracle or DB2 datastore, you must identify tablespaces for data, indexes, blobs, and a temporary tablespace.
12. To avoid overwriting macros or administration links, for each object with a warning next to it in the **Object Mapping** page, type a new name for the target object directly into the target column.
13. Optionally, if you are importing a model without data, select the option to automatically go to production with all imported applications during the import process.
14. If you are overwriting objects, you will be prompted to confirm the import, to continue, click **Yes**.
15. Click **Finish**.
16. Click **OK**.

The import request starts on the server.

You can view the progress of the export in the **Monitoring Console** on the **Deployments** tab.

If you did not set the job server cluster in the **Map All** dialog, refresh the console after the transfer is complete and add any newly created applications to a job server cluster.

Tip: During the import process, some application options are excluded from the transfer because they do not apply to the new application location, for example, display names, backup location, and publish options are excluded. If these options are required, you can include them by modifying the `AdminOptions` to exclude during `Limited transfer` or `AdminOptions` to exclude during `Full transfer` resource values in the `<install_location>\bin\epPNHelperResource.xml` file.

Recommendation - Test the Upgraded Content

After you import the packages from the deployment archive, you can check that all the entries were deployed successfully in the target environment.

We recommend that you test your upgraded content by doing the following:

- ☐ View the status of existing deployments.
- ☐ Ensure that the correct packages and folders were imported, along with their contents.
- ☐ Test models.
- ☐ Test applications.
- ☐ Repair or exclude models that do not operate correctly.
- ☐ Test the repaired models by running them again on the test system.

Troubleshoot any issues, and contact IBM Cognos Software Services about unresolved upgrade issues.

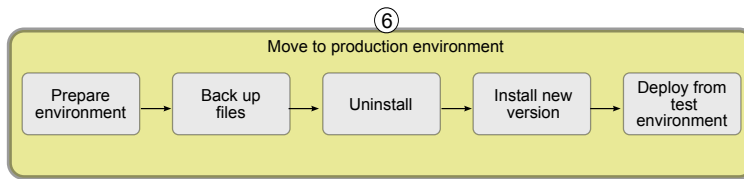
- ☐ Revise the upgrade plan to include adaptations that you made during the trial upgrade.

For more information, see the IBM Cognos Contributor *Administration Guide*.

Moving to the Production Environment

When all issues that you discovered during the trial upgrade are resolved, you are ready to begin the full upgrade in your production environment. Your upgrade plan will provide the details for each step of the full upgrade.

The following diagram shows the high level steps in the process of moving upgraded applications to a production environment. After preparing the production environment and backing up data and configuration files, you can uninstall the older version of the software, and install the new version in the same location. Then, you can deploy the content from your test environment.



Use the following checklist to guide you through the process of moving to a production environment:

☐ Prepare the production environment.

- Back up files and data.

You may have modified files other than those in the configuration folder. If so, you should also back up the additional files before upgrading.

When you back up the configuration data, store it in a secure directory. You must protect the directory from unauthorized or inappropriate access.

- Install your new release system in the production environment.

If you install the new software from the test environment to the same location as the existing software, you must first uninstall the existing software.

- Configure the system.

☐ Manually configure customization.

- If you manually edited any configuration files, the changes will be overwritten during the upgrade. You must reapply the changes. You should keep a record of any customizations to ensure that they can be reapplied after upgrading. You should also back up these files so that you can restore the original version if necessary.
- The IBM Cognos 8 presentation service supports automatic upgrade of some system.xml files. If you made many customization changes to system.xml files, you can use this automatic upgrade feature instead of reapplying the changes manually after upgrading. The system.xml files are overwritten during the installation of IBM Cognos 8. Therefore, you must back up the customized versions of these files and then copy them to the directory after upgrading IBM Cognos 8. The automatic upgrade will be applied when you start the IBM Cognos 8 service.
- The system.xml files for which automatic upgrade is supported are in the following directories: *c8_location/templates/ps*, *c8_location/templates/ps/portal*, and *c8_location/templates/ps/qs*.
- **Note:** The recommended method to upgrade customized files is to manually reapply changes after the new software is installed. Use automatic upgrade of system.xml files only when you have made a large number of customizations to these files.

☐ Start deployment on the production system.

Upgrading Planning Administration Domains

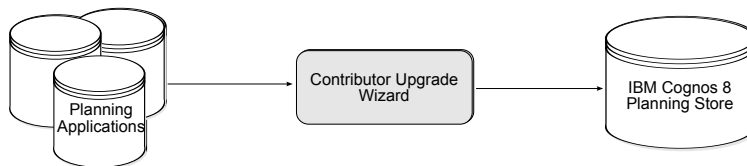
Use the Planning Administration Domain wizard to upgrade version 7.3 or 8.1 Planning Application Domains to version 8.4, as shown in the following diagram.



For more information, see the "Upgrade the Planning Application Domain" section of the Contributor *Administration Guide*.

Upgrading Planning Applications

Use the Upgrade wizard to upgrade version 7.2, 7.3 or 8.1 Planning applications, as shown in the following diagram.



For more information, see the "Upgrade Contributor Applications" section of the Contributor *Administration Guide*.

Upgrade Analyst Security and Library Files

If you use Analyst models in your Contributor applications, then you need to upgrade Analyst security and library files.

Upgrading Analyst security and library files involves the following tasks:

- ☐ Create backup copies of your IBM Cognos Planning - Analyst configuration files and data directories from the existing installation.
- ☐ Uninstall previous Analyst clients.
- ☐ Install IBM Cognos 8 Planning - Administration components, including Analyst.
- ☐ Upgrade Analyst libraries, user classes, users, and groups.

Upgrade Analyst Libraries, User Classes, Users, and Groups

You can upgrade all existing libraries, user classes, users, and groups at the same time, or individually.

Note: If you want to upgrade users and groups from a Series 7 namespace, use IBM Cognos Configuration to connect to the Series 7 namespace. Then, start Analyst and add the users, groups and roles that you want to use.

Steps

1. Start Analyst.
2. Upgrade Analyst by doing one of the following:
 - To upgrade libraries, user classes, users, and groups at the same time, from the **File** menu, select **Administration, Upgrade, Existing File System**, browse to find your existing filesys.ini file, and click **Open**.
 - To upgrade libraries, from the **File** menu, select **Administration, Upgrade, Existing Libraries**, browse to find your existing Libs.Tab file, and click **Open**.
 - To upgrade user classes, from the **File** menu, select **Administration, Upgrade, Existing User Classes**, browse to find your existing usersclasses.Tab file and click **Open**.
 - To upgrade existing native security to Access Manager, from the **File** menu, select **Administration, Upgrade, Existing Native Users and Groups**, browse to find your existing existingusers.Tab file, and click **Open**.

The files are converted automatically to 8.4 format, after which they can no longer be opened in a previous version of Analyst.

Upgrading a Test or Development Environment

You can quickly upgrade your test or development environment using an in-place upgrade.

Note: Never use an in-place upgrade for your production environment.

If you set your database connection properties for your new version of Planning to use your version 8.2 or 8.3 planning store, you are prompted to upgrade the planning store to version 8.4 when you open Contributor Administration the first time. Upgrading the planning store also upgrades all of your applications in the Planning Administration Domain.

If you have version 8.2 or 8.3 applications that are not in your Planning Administration Domain, you can upgrade these applications by linking to them in the Contributor Administration Console.

Upgrading From Versions 7.2, 7.3, or 8.1

The IBM Cognos 8 Planning upgrade process for versions 7.2, 7.3, and 8.1 involves the following stages:

- ☐ [Plan the upgrade.](#)
- ☐ Design, install, and configure the test environment.

For more information, see ["Installation Options" \(p. 21\)](#) or the IBM Cognos 8 Planning *Architecture and Deployment Guide*.

- ❑ Assign roles to Contributor administrators and users.
 - assign Contributor Administration users and Analyst administrators to the Planning Rights Administrator role
 - add Contributor users to the Planning Contributor Users role

For more information, see the IBM Cognos 8 *Administration and Security Guide* or the IBM Cognos Contributor *Administration Guide*.

- ❑ [Upgrade Analyst security and library files.](#)

- ❑ Upgrade planning applications in the test environment.

For more information, see [Upgrading Planning Administration Domains](#).

- ❑ Upgrade the Planning Administration Domain.

For more information, see [Upgrading Planning Applications](#).

- ❑ Test all components to ensure that the applications upgraded successfully.

- ❑ Install and configure the new production environment.

- ❑ Export the test planning environment to the new production environment.

- ❑ Export the deployment package for Framework Manager or Event Studio objects.

For more information, see the IBM Cognos 8 *Administration and Security Guide*.

- ❑ Import the planning environment to the new production environment.

For more information, see the IBM Cognos 8 Planning Contributor *Administration Guide*.

- ❑ Import the deployment package for Framework Manager or Event Studio objects to the production environment.

For more information, see the IBM Cognos 8 *Administration and Security Guide*.

Chapter 6: Installing and Configuring IBM Cognos 8 Planning on One Computer

IBM Cognos 8 Planning requires the installation of server components and client components. These installations are suitable when you are setting up a test or evaluation environment, or for small production environments. This installation is the quickest and easiest way to get started.

The tasks that you must perform to install IBM Cognos 8 Controller on one computer are as follows:

- ❑ [Install IBM Cognos 8 Planning.](#)
- ❑ [Start IBM Cognos Configuration.](#)
- ❑ [Set database connection properties for the content store.](#)
- ❑ [Set database connection properties for the Planning store.](#)
- ❑ [Configure environment properties.](#)
- ❑ Enable security.
- ❑ Configure the Web Server.
- ❑ [Start the IBM Cognos 8 Planning services.](#)
- ❑ [Install the clients.](#)

Note: Install IBM Cognos 8 components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.

After you complete these installation and configuration tasks, you can perform additional configuration tasks, and change the IBM Cognos 8 Controller default behavior to better suit your environment.

If you no longer require IBM Cognos 8 Controller, you can [uninstall](#) all IBM Cognos 8 Controller components.

Install IBM Cognos 8 Planning

Use the IBM Cognos 8 Planning Server CD installation wizard to install the gateway, Planning Server, and Content Manager components. Installing all server components on the same computer is intended for proof of concept installations or demonstration environments.

The IBM Cognos 8 Planning Server CD also allows you to install a network installation point ([p. 116](#)).

Ensure that you have administrator privileges for the computer on which you are installing. Also ensure that your computer has a TEMP system variable that points to the directory where you want

to store temporary files. During installation, files from the CD are temporarily copied to this directory.

If you intend to distribute IBM Cognos 8 Planning, you can start your installation process by installing the server components on a single computer. After you verify that it is running, you can add server components as required. For example, you can install additional Planning Servers to your initial installation. Then, after you have the Planning Servers running, you can turn off some of the services on the computer with Content Manager installed on it to optimize its performance.

Do not install IBM Cognos 8 Planning server components on a computer running Windows Vista.

Steps

1. If you are installing to a directory with other IBM Cognos 8 components, stop the IBM Cognos 8 service.

2. Insert the IBM Cognos 8 Planning Server CD or go to the installation source file directory.

The **Welcome** page of the installation wizard appears when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click `issetup.exe`.

3. Select the language to use for the installation.

The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

4. In the **Component Selection** screen, select all components, except for **Analyst UNC Connection Point**.

The **Analyst UNC Connection Point** option allows you to create a network connection so that multiple users can access shared libraries. For more information, see "[Install an Analyst Network Connection Point](#)" (p. 116).

5. Follow the directions in the installation wizard to copy the required files to your computer.

If an older version of the Microsoft Windows Installer Tool is installed on your computer, you are prompted to manually install Microsoft SOAP Toolkit before you configure your IBM Cognos 8 Planning environment.

If you are installing in a directory that already has other IBM Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

6. In the **Finish** page of the installation wizard,

- If you want to configure Content Manager immediately, click **Start IBM Cognos Configuration**.
- If you want to see late-breaking information about IBM Cognos components, click **View the README**.

7. Click **Finish**.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos 8 components and to start and stop IBM Cognos services.

Step

- From the **Start** menu, click **Programs, IBM Cognos 8, IBM Cognos Configuration**.

Set Database Connection Properties for the Content Store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

Ensure that you used one of the supported database servers to create the content store.

Note: Some database servers are available with advanced features. When you select an advanced database option, IBM Cognos 8 uses features of the database server to manage the connection. For example, if you select the advanced Oracle database, IBM Cognos 8 uses enterprise-oriented Oracle features to

- select a listener
- switch to another listener if the first listener fails
- automatically reconnect to the database if the connection fails
- balance connection requests among listeners
- and balance connection requests among dispatchers.

IBM Cognos 8 requires the TCP/IP protocol to access data and the content store. Ensure that the database server has the protocol set to TCP/IP.

Steps for Microsoft SQL Server

1. In the IBM Cognos Configuration Explorer window, under **Data Access, Content Manager**, click **Content Store**.

The connection properties are shown.

2. Type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type `localhost\instance1`. If no instance name property is specified, a connection to the default instance is created.

Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

`jdbc:JSQConnect://localhost\\instance1/user=sa/more properties as required`

3. Specify a user ID and password:

- Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
- Type the appropriate values and click **OK**.

4. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

5. Test the connection between Content Manager and the content store.

Tip: In the **Explorer** window, right-click the new database and click **Test**.

Content Manager connects to the database, checks the database permissions, and creates and populates a table. Content Manager uses the same table each time you test the connection.

Steps for Oracle, DB2, or Sybase

1. In the IBM Cognos Configuration **Explorer** window, under **Data Access, Content Manager**, right-click **Content Store** and click **Delete**.

This deletes the default resource, Microsoft SQL Server.

2. Right-click **Content Manager**, and then click **New resource, Database**.

3. In the **Name** box, type a name for the resource.

4. In the **Type** box, select the type of database and click **OK**.

Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

5. In the **Properties** window, provide values depending on your database type:

- If you use a DB2 database, for the **Database name** property, type the database alias.
- If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.
- If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an example:

`(description=(address=(host=myhost)(protocol=tcp)(port=1521) (connect_data=(sid=(orcl)))))`

- If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.

6. Specify a user ID and password:

- Click the **Value** box next to the **User ID and password** property, and then click the edit button when it appears.
 - Type the appropriate values and click **OK**.
7. From the **File** menu, click **Save**.
The logon credentials are immediately encrypted.
 8. Test the connection between Content Manager and the content store.
Tip: In the **Explorer** window, right-click the new database and click **Test**.
Content Manager connects to the database, checks the database permissions, and creates and populates a table. Content Manager uses the same table each time you test the connection.

Content Manager can now create the required tables in the content store when you start the IBM Cognos 8 service for the first time. If you do not specify the connection properties correctly, you cannot start the IBM Cognos 8 service.

Set Database Connection Properties for the Planning Store

You must specify database connection information for the planning store. The planning store can be the same database as the content store, or it can be a different database. The database must be created before you can connect to it.

Note: Some database servers are available with advanced features. When you select an advanced database, IBM Cognos 8 uses features of the database server to manage the connection. If you select the advanced Oracle database, for example, IBM Cognos 8 uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.

Steps

1. In the **Explorer** window, under **Data Access**, right-click **IBM Cognos Planning**, and click **New resource, Database**.
2. In the **Name** box, type a name for the resource.
3. In the **Type** box, select the type of database and click **OK**.

Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

4. In the **Properties** window, provide values depending on your database type:
 - If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.
For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type `localhost\instance1`. If no instance name property is specified, a connection to the default instance is created.

Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

```
jdbc:JSQLConnect://localhost\instance1/user=sal/more properties as required
```

- If you use a DB2 database, for the **Database name** property, type the database alias.
- If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.
- If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an example:

```
(description=(address=(host=myhost)(protocol=tcp)(port=1521) (connect_data=(sid=(orcl)))))
```

5. To set the user ID and password for the database:
 - Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
 - Type the appropriate values and click **OK**.

6. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

Configure Environment Properties

The IBM Cognos 8 service runs as a service in an IBM Cognos 8 dispatcher. The dispatcher runs in a Tomcat servlet container. The Planning Server service runs as a Windows service. By default the IBM Cognos 8 dispatcher uses port number 9300 for communications, and the Planning Server service uses port 9900. You can change these port numbers to any available port number.

Steps

1. In the IBM Cognos Configuration **Explorer** window, click **Environment**.
2. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
3. Specify the URIs for the other Content Manager computers:
 - In the **Value - Content Manager URIs** dialog box, click **Add**.
 - In the blank row of the table, click and then type the full URI of the Content Manager computer.

Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.

- Repeat the previous two bulleted steps for each URI to be added.
Important: You must include all Content Manager URIs in the list.
 - Click **OK**.
4. In the **Explorer** window, under **Security, Cryptography**, click **IBM Cognos**, the default cryptographic provider.
 5. Under the **Certificate Authority settings** property group, type a **Password**.
 6. In the **Explorer** window, under **Security**, click **Cryptography**.
 7. In the **Properties** window, under **CSK settings**, set **Store symmetric key locally** to **True**.
 8. From the **File** menu, click **Save**.

If you configured IBM Cognos 8 with standby Content Manager computers and you use the default CGI gateway, you must now configure IBM Cognos 8 to use an ISAPI gateway. For more information, see ["Changing the Gateway" \(p. 135\)](#).

Enable Security

IBM Cognos 8 Planning requires that users log in. This ensures that users only see parts of budgets or plans for which they are responsible.

By default, IBM Cognos 8 Planning allows anonymous access to the Web portal. You must disable anonymous access and configure IBM Cognos 8 Planning to use an authentication provider before users can access any of the client applications or the portal.

Steps

1. In the IBM Cognos Configuration **Explorer** window, click **Security, Authentication, IBM Cognos**.
2. Click the **Value** box for **Allow Anonymous Access?**, and select **False**.
3. Right-click **Authentication**, and click **New Resource, Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

6. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

For more information about configuring IBM Cognos 8 to use an authentication provider, see ["Configuring IBM Cognos 8 Components to Use an Authentication Provider" \(p. 147\)](#).

7. From the **File** menu, click **Save**.

Configure the Web Server

You must create virtual directories to connect to the IBM Cognos 8 portal and for client applications to be able to connect to the server.

Step

- Create the following virtual directories:

Alias	Location	Permission
cognos8	<i>c8_location</i> /webcontent	Read
cognos8/cgi-bin	<i>c8_location</i> /cgi-bin	Execute

Note: The cogrcp folder, located in *c8_location*/planning/contributor must have **Scripts only** execute permissions.

You can use a name other than cognos8 in the aliases. However, you must use cgi-bin as the second part of the alias. If you use an alias other than cognos8 you must change the virtual directory in the **Gateway URI** property to match your alias.

For Apache Web Server, ensure that you define the cognos8/cgi-bin alias before the cognos8 alias in the httpd.conf file located in the *Apache_installation*/conf directory. You must define the cognos8/cgi-bin alias as a ScriptAlias.

Start the IBM Cognos 8 Planning Services

After you have set the database connection properties for the content store and planning store, you can start the IBM Cognos 8 Planning services.

Step

- From the **Actions** menu, click **Start**.

This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Uninstalling IBM Cognos 8

It is important to use uninstall programs to completely remove all files and modifications to system files.

Uninstall IBM Cognos 8 on Windows

If you no longer require IBM Cognos 8 or if you are upgrading, uninstall all IBM Cognos 8 components and the IBM Cognos 8 service.

If you installed more than one component in the same location, the uninstall wizard lets you choose the packages to uninstall. All components of the package will be uninstalled. You must repeat the uninstallation process on each computer that contains IBM Cognos 8 components.

It is not necessary to back up the configuration and data files on Windows. These files are preserved during the uninstallation.

We recommend that you close all programs before you uninstall IBM Cognos 8. Otherwise, some files may not be removed.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them using Windows Explorer.

Important: Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos 8 and you want to use the configuration data with the new version.

Steps

1. From the **Start** menu, click **Programs, IBM Cognos 8, Uninstall IBM Cognos 8**.

The **Uninstall** wizard appears.

Tip: IBM Cognos 8 is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.

2. Follow the instructions to uninstall the components.

The `cognos_uninst_log.htm` file records the activities that the Uninstall wizard performs while uninstalling files.

Tip: To find the log file, look in the Temp directory.

3. Delete all temporary Internet files.

For more information, see your Web browser documentation.

Chapter 7: Installing and Configuring IBM Cognos 8 Planning on Different Computers

IBM Cognos 8 Planning requires the installation of server components and client components.

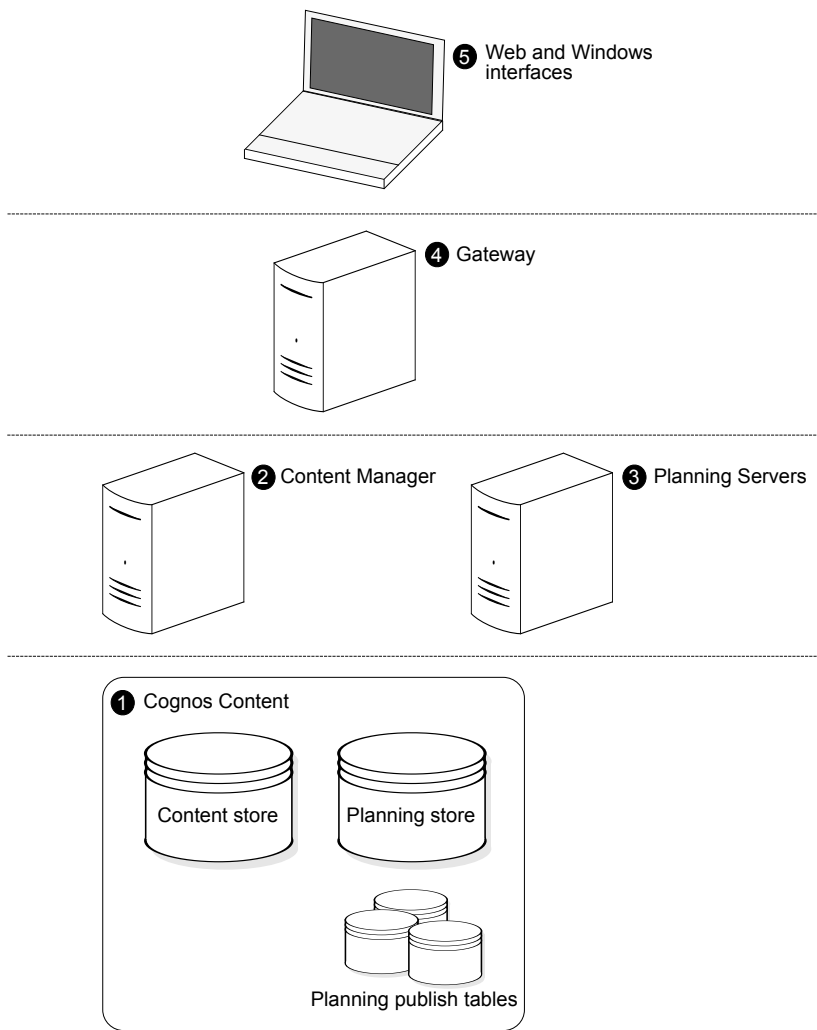
The IBM Cognos 8 Planning server components include the following:

- [Content Manager](#)
- [Planning Server](#)
- [Planning Gateway](#)

You must install the gateway on a computer that is also running a Web server.

To improve scalability in an environment that serves many users, you can install the Planning Server component on multiple computers dedicated to processing incoming requests. This strategy distributes and balances loads among the computers, and provides better accessibility, throughput, and failover support than installing on a single computer.

The following diagram shows the IBM Cognos 8 Planning components, and the order in which they should be configured and started. You must configure and start Content Manager before you can start a Planning Server.



1. [Set up your environment for IBM Cognos content data stores](#), such as creating the content store and the planning store
2. [Install and configure Content Manager](#)
3. [Install and configure the Planning Server](#)
4. [Install the gateway and create virtual directories](#)
5. [Install the clients.](#)

Note: Install IBM Cognos 8 components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.

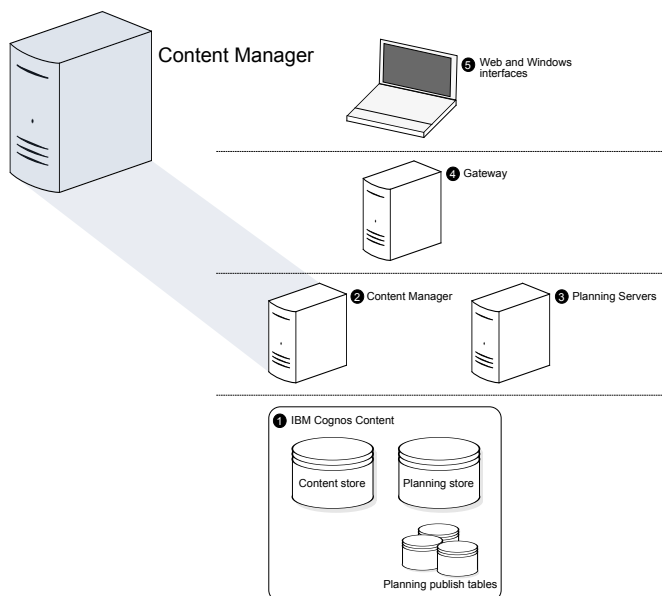
After you complete these installation and configuration tasks, you can perform additional configuration tasks, and change the IBM Cognos 8 Controller default behavior to better suit your environment.

If you no longer require IBM Cognos 8 Controller, you can [uninstall](#) all IBM Cognos 8 Controller components.

The IBM Cognos 8 Planning server components cannot be installed on computers running Windows Vista.

Install and Configure Content Manager

Content Manager stores and manages IBM Cognos content, including user permissions. Content Manager must be configured, running, and accessible before you configure other computers in your IBM Cognos environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other IBM Cognos computers.



After you install Content Manager, you must perform the following tasks to configure and start the Content Manager services.

- ☐ [Start IBM Cognos Configuration](#)
- ☐ [Set database connection properties for the content store](#)
- ☐ [Configure environment properties for Content Manager](#)
- ☐ [Enable security](#)
- ☐ [Start Content Manager](#)
- ☐ [Test the Content Manager installation](#)

Steps

1. If you are installing to a directory with other IBM Cognos 8 components, stop the IBM Cognos 8 service.
2. Insert the IBM Cognos 8 Planning Server CD or go to the installation source file directory.

The **Welcome** page of the installation wizard appears when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click issetup.exe.

3. Select the language to use for the installation.

The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

4. In the **Component Selection** screen, select **Content Manager**.

If you are installing it in a directory that contains other IBM Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

5. In the **Finish** page of the installation wizard,
 - If you want to configure Content Manager immediately, click **Start IBM Cognos Configuration**.
 - If you want to see late-breaking information about IBM Cognos components, click **View the Readme**.
6. Click **Finish**.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos 8 components and to start and stop IBM Cognos services.

Step

- From the **Start** menu, click **Programs, IBM Cognos 8, IBM Cognos Configuration**.

Set Database Connection Properties for the Content Store

You must specify the database server information to ensure that Content Manager can connect to the database that you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

Ensure that you used one of the supported database servers to create the content store.

Note: Some database servers are available with advanced features. When you select an advanced database, IBM Cognos 8 uses features of the database server to manage the connection. If you select the advanced Oracle database, for example, IBM Cognos 8 uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.

IBM Cognos 8 requires the TCP/IP protocol to access data and the content store. Ensure that the database server has the protocol set to TCP/IP.

Steps for Microsoft SQL Server

1. In the IBM Cognos Configuration **Explorer** window, under **Data Access, Content Manager**, click **Content Store**.

The connection properties are shown.

2. Type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type `localhost\instance1`. If no instance name property is specified, a connection to the default instance is created.

Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

```
jdbc:SQLConnect://localhost\instance1/user=sa/more properties as required
```

3. Specify a user ID and password:
 - Click the **Value** box next to the **User ID and password** property, and then click the edit button when it appears.
 - Type the appropriate values and click **OK**.
4. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

5. Test the connection between Content Manager and the content store.

Tip: In the **Explorer** window, right-click the new database and click **Test**.

Content Manager connects to the database, checks the database permissions, and creates and populates a table. Content Manager uses the same table each time you test the connection.

Steps for Oracle or DB2

1. In the IBM Cognos Configuration **Explorer** window, under **Data Access, Content Manager**, right-click **Content Store** and click **Delete**.

This deletes the default resource, Microsoft SQL Server.

2. Right-click **Content Manager**, and then click **New resource, Database**.
3. In the **Name** box, type a name for the resource.
4. In the **Type** box, select the type of database and click **OK**.

Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

5. In the **Properties** window, provide values depending on your database type:
 - If you use a DB2 database, for the **Database name** property, type the database alias.
 - If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.

- If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an example:

```
(description=(address=(host=myhost)(protocol=tcp)(port=1521) (connect_data=(sid=(orcl)))))
```

6. Specify a user ID and password:

- Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
- Type the appropriate values and click **OK**.

7. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

8. Test the connection between Content Manager and the content store.

Tip: In the **Explorer** window, right-click the new database and click **Test**.

Content Manager connects to the database, checks the database permissions, and creates and populates a table. Content Manager uses the same table each time you test the connection.

Content Manager can now create the required tables in the content store when you start the IBM Cognos 8 service for the first time. If you do not specify the connection properties correctly, you cannot start the IBM Cognos 8 service.

Configure Environment Properties for Content Manager

Content Manager runs as a service in an IBM Cognos 8 dispatcher. The dispatcher runs in a Tomcat servlet container. By default the IBM Cognos 8 dispatcher uses port number 9300 for communications. You can change this port number.

Content Manager also creates security keys that allow only authorized servers to communicate with it. If you are installing server components on different computers, you must ensure that you set the same password for the **Certificate Authority settings** in IBM Cognos Configuration.

Steps

1. In the IBM Cognos Configuration **Explorer** window, click **Environment**.
2. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
3. Specify the URIs for the other Content Manager computers:
 - In the **Value - Content Manager URIs** dialog box, click **Add**.
 - In the blank row of the table, click and then type the full URI of the Content Manager computer.

Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.
 - Repeat the previous two bulleted steps for each URI to be added.

Important: You must include all Content Manager URIs in the list.

- Click **OK**.
4. In the **Explorer** window, under **Security, Cryptography**, click **IBM Cognos**, the default cryptographic provider.
 5. Under the **Certificate Authority settings** property group, type a **Password**.
 6. In the **Explorer** window, under **Security**, click **Cryptography**.
 7. In the **Properties** window, under **CSK settings**, set **Store symmetric key locally** to **True**.
 8. From the **File** menu, click **Save**.

If you configured IBM Cognos 8 with standby Content Manager computers and you use the default CGI gateway, you must now configure IBM Cognos 8 to use an ISAPI gateway. For more information, see ["Changing the Gateway" \(p. 135\)](#).

Enable Security

IBM Cognos 8 Planning requires that users log in. This ensures that users only see parts of budgets or plans for which they are responsible.

By default, IBM Cognos 8 Planning allows anonymous access to the Web portal. You must disable anonymous access and configure IBM Cognos 8 Planning to use an authentication provider before users can access any of the client applications or the portal.

Steps

1. In the IBM Cognos Configuration **Explorer** window, click **Security, Authentication, IBM Cognos**.
2. Click the **Value** box for **Allow Anonymous Access?**, and select **False**.
3. Right-click **Authentication**, and click **New Resource, Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

6. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

For more information about configuring IBM Cognos 8 to use an authentication provider, see ["Configuring IBM Cognos 8 Components to Use an Authentication Provider" \(p. 147\)](#).

7. From the **File** menu, click **Save**.

Start Content Manager

After you have set the database connection properties for the content store, you can start the Content Manager computer.

Step

- From the **Actions** menu, click **Start**.

It may take a few minutes for the IBM Cognos 8 service to start.

This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Test the Content Manager Installation

You can test the installation using a Web browser.

Steps

1. Open a Web browser.
2. Test that Content Manager is running by typing the **Content Manager URIs** value from IBM Cognos Connection. For example,

`http://hostname:port_number/p2pd/servlet`

The **State** value should be **Running**.

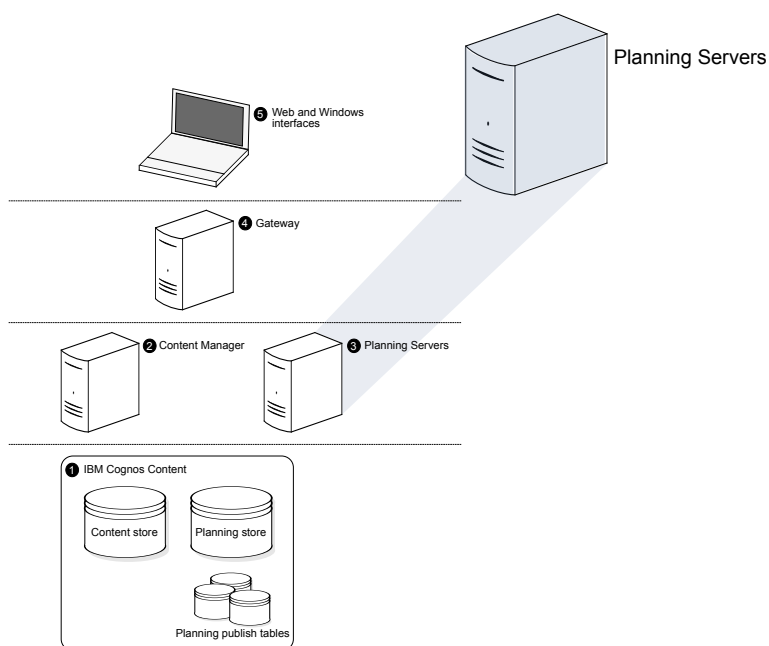
Install and Configure the Planning Server

Planning Servers run job-based administration task, such as publishing and reconciliation tasks, manage communications with IBM Cognos 8 Planning clients and IBM Cognos 8 Business Intelligence components. Depending on your environment, you may need to install more than one Planning Server.

To improve scalability in an environment that serves many users, you can install the Planning Server component on multiple computers dedicated to processing incoming requests. This strategy distributes and balances loads among the computers, and provides better accessibility, throughput, and failover support than installing on a single computer.

After you install the Planning Servers, you can configure specific roles for each server. For more information, see ["Enabling Only Services That are Required" \(p. 93\)](#).

Ensure that you have administrator privileges for the Windows computer on which you are installing. Also ensure that your computer has a TEMP system variable that points to the directory where you want to store temporary files. During installation, files from the CD are temporarily copied to this directory.



After you install the Planning Server, you must perform the following tasks to configure and start the services.

- ☐ [Configure environment properties for the Planning Server](#)
- ☐ [Set database connection properties for the planning store](#)
- ☐ [Start the Planning Server](#)

Steps

1. If you are installing to a directory with other IBM Cognos 8 components, stop the IBM Cognos 8 service.
2. Insert the IBM Cognos 8 Planning Server CD or go to the installation source file directory.
The **Welcome** page of the installation wizard appears when you insert the CD.
If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click issetup.exe.
3. Select the language to use for the installation.
The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.
4. In the **Component Selection** screen, select **Planning Server**.
If you are installing it in a directory that contains other IBM Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.
5. In the **Finish** page of the installation wizard,
 - If you want to configure Content Manager immediately, click **Start IBM Cognos Configuration**.

- If you want to see late-breaking information about IBM Cognos components, click **View the Readme**.

6. Click **Finish**.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos 8 components and to start and stop IBM Cognos services.

Step

- From the **Start** menu, click **Programs, IBM Cognos 8, IBM Cognos Configuration**.

Set Database Connection Properties for the Planning Store

You must specify database connection information for the planning store. The planning store can be the same database as the content store, or it can be a different database. You must create the database you will use for the planning store before you can connect to it.

If you install multiple Planning Servers in your environment, you must set the connection properties for the planning store on each Planning Server computer.

The planning store can be on a Microsoft SQL Server, Oracle, or DB2 database.

Note: Some database servers are available with advanced features. When you select an advanced database, IBM Cognos 8 uses features of the database server to manage the connection. If you select the advanced Oracle database, for example, IBM Cognos 8 uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.

Steps

1. In the **Explorer** window, under **Data Access**, right-click **IBM Cognos Planning**, and click **New resource, Database**.
2. In the **Name** box, type a name for the resource.
3. In the **Type** box, select the type of database and click **OK**.

Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

4. In the **Properties** window, provide values depending on your database type:
 - If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type `localhost\instance1`. If no instance name property is specified, a connection to the default instance is created.

Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

```
jdbc:SQLConnect://localhost\instance1/user=salmore properties as required
```

- If you use a DB2 database, for the **Database name** property, type the database alias.
- If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.
- If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an example:

```
(description=(address=(host=myhost)(protocol=tcp)(port=1521) (connect_data=(sid=(orcl)))))
```

5. To set the user ID and password for the database
 - Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
 - Type the appropriate values and click **OK**.
6. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

Configure Environment Properties for the Planning Server

The Planning Server must know the location of the gateway computer and the Content Manager computer. You can also configure the port numbers that the IBM Cognos services use on the Planning Server computer.

Steps

1. In the IBM Cognos Configuration **Explorer** window, click **Environment**.
2. In the **Properties** window, click the value for **Gateway URI** and then specify the URI for a gateway computer.
3. In the **Properties** window, click the value for **Content Manager URIs**, and then click the edit button.
4. Specify the URI for the Content Manager computer:
 - In the **Value - Content Manager URIs** dialog box, type the URI of the Content Manager computer.

If you are installing multiple Content Managers for failover protection, you must list all Content Manager URIs on each Planning Server computer.

- Click **OK**.
5. To change the port numbers that the IBM Cognos 8 services use, edit each of the following to be the same port number.
 - **External dispatcher URI**
 - **Internal dispatcher URI**
 - **Dispatcher URI for external applications**
 6. To change the port numbers that the Planning Server uses, in the IBM Cognos Configuration **Explorer** window, click **Environment, Planning, Planning Server**, and type the new port number.
 7. In the **Explorer** window, under **Security, Cryptography**, click **IBM Cognos**, the default cryptographic provider.
 8. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
 9. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
 10. From the **File** menu, click **Save**.

Configuring Role-based Planning Servers

If you install multiple Planning Servers, you can configure each server to perform a specific role. You set roles by enabling and disabling services that are run by the dispatcher service (p. 93).

The planning server roles are determined by the services running on that computer, which can include a planning job service, a planning data service, a planning administration service, and a planning Web service.

Each server must have the dispatcher service enabled and running. However, you can choose which Planning services you want running on each computer. There must also be at least one Planning Server running all non-Planning services, such as the data movement service, event management service, report service, and so on.

Planning Job Servers

Planning job servers run job-based administrative tasks, such as publishing and reconciliation tasks, and divide work among other available job servers.

Planning job servers implement a proprietary job-server clustering technique that allows you to allocate or distribute work to individual job servers. You can also then distribute job-based work as appropriate for a group of applications and macros over a group of job servers belonging to a cluster. You can allocate a single cluster of job servers to monitor many applications to make most efficient use of all job server resources. Alternatively, you can dedicate a single job server or job server cluster to a specific application to ensure that resources are available.

In most cases, we recommend that planning job servers have only the dispatcher and the planning job services enabled. By having many planning job servers, you can distribute the work load. We

recommend that you have more planning job servers than other role-based planning servers because job servers consume the most resources.

Planning Data Servers

Planning data servers manage communications between IBM Cognos 8 Business Intelligence components, such as Report Studio and Analysis Studio, and Contributor applications to provide real-time IBM Cognos 8 reporting and analysis activities.

Planning Administration Servers

Planning administration servers manage communications with Contributor Administration and performs other administrative tasks.

Contributor Administration users connect to the Planning administration server through the gateway.

Planning Web Servers

Planning web servers manage Contributor Web Client and Contributor *for Microsoft Excel* client communications.

The gateway manages client connectivity in the Web tier, and the planning web service manages client connectivity in the application tier. Clients communicate directly with the gateway, and with the planning web server through the dispatcher. The planning web server communicates with the planning store and sends data back to the clients through the gateway.

Enabling Only Services That are Required

If some IBM Cognos 8 services are not required in your environment, you can disable them to increase the performance of other services.

For example, if you are using a job server to only run planning jobs, that job server does not need to run reports. If you disable the report service, the performance of the job server will improve.

Notes:

- The presentation service must remain enabled on at least one computer in your IBM Cognos 8 Planning environment.
- If you have IBM Cognos 8 Business Intelligence installed and you want to use Query Studio, you must ensure the presentation service is enabled on at least one server.
- If you have IBM Cognos 8 Business Intelligence installed and you want to use Analysis Studio, you must enable the report service on at least one server.
- If some IBM Cognos 8 components are not installed on a computer, disable the services associated with the missing components. Otherwise the IBM Cognos 8 components will randomly fail.

The services are listed in the following table.

Service	Purpose
Agent service	Runs agents. If the conditions for an agent are met, the agent service asks the monitoring service to run the tasks.
Batch report service	Manages background requests to run reports and provides output on behalf of the monitoring service.
Content Manager service	<p>Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy.</p> <p>Also performs content store management functions, such as import and export.</p>
Data movement service	Runs data movement tasks in IBM Cognos 8. Data movement tasks, such as Builds and JobStreams, are created in Data Manager Designer and published to IBM Cognos 8.
Delivery service	Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, agent service, or data integration service.
Event management service	Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, deployment imports and exports, and metrics.
Job service	Runs jobs by signaling the monitoring service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.
Monitoring service	<p>Monitors and runs tasks that are scheduled, submitted for running at a later time, or run as a background task.</p> <p>Assigns a target service to handle a scheduled task. For example, the monitoring service can ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent.</p> <p>Creates history objects within Content Manager and manages failover and recovery for running entries.</p>
Presentation service	<p>Transforms generic XML responses from another service into output format, such as HTML, for the portal user interface.</p> <p>Provides presentation, navigation, and administration capabilities in IBM Cognos Connection.</p>

Service	Purpose
Report service	Manages interactive requests to run reports and provides output for a user in IBM Cognos Connection or a studio.
Planning job service	Manages communications with the Planning Job Server subsystem.
Planning Web service	Manages communications with Contributor Web and Contributor <i>for Microsoft Excel</i> users.
Planning administration console service	Manages communication with Contributor Administration.
Planning data service	Manages communications for real-time reporting from Contributor plan data in IBM Cognos 8.

Use the following steps to enable or disable the services you want running on each Planning Server computer. Ensure that you do not disable the dispatcher service.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **IBM Cognos 8 service**.
3. In the **Properties** window, click the **Value** next to the service that you want to disable or enable.
By default, all services are enabled.
4. Click the appropriate state for the services:
 - To disable the service, click **False**.
 - To enable the service, click **True**.

For example:

- for a Planning job server, you must enable the dispatcher service, the monitoring service, and the Planning job service. All other services can be disabled.
- for a Planning data server, you must enable the dispatcher service, the monitoring service, and the Planning data service.
- for a Planning administration server, you must enable the dispatcher service, the monitoring service, and the Planning administration console service.
- for a Planning Web server, you must enable the dispatcher service, the monitoring service, and the Planning Web service.

If you are configuring role-based Planning servers, you must also ensure that at least one Planning server has all the other IBM Cognos 8 services running.

5. From the **File** menu, click **Save**.

Start the Planning Server

After you have set the environment properties and database connection properties for the planning store, you can start the Planning Server computer.

Content Manager must be running before you start the Planning Server services.

Step

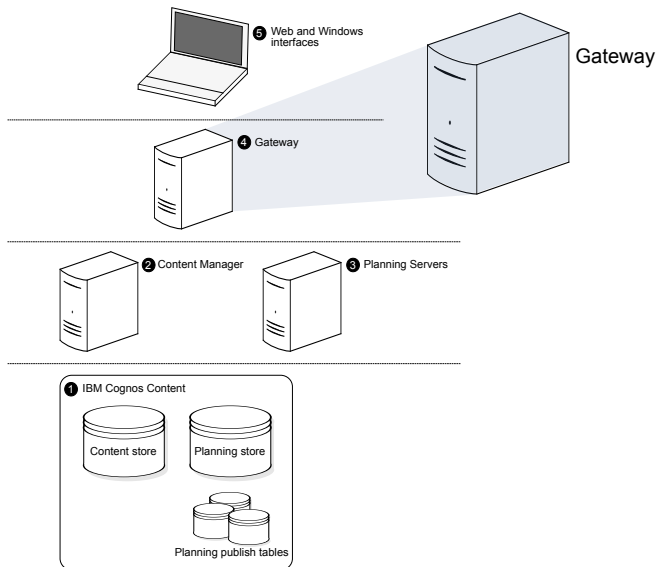
- From the **Actions** menu, click **Start**.

It may take a few minutes for the IBM Cognos 8 service and IBM Cognos 8 Planning service to start.

This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Install the Gateway

You must install the IBM Cognos 8 Planning gateway on a Web server computer. You can install the gateway on one or more computers, depending on your environment.



After you install the Planning Gateway, you must

- [configure environment properties for the gateway](#)
- [configure your Web server](#)

If you are installing IBM Cognos 8 Planning into an environment where you have another IBM Cognos 8 product installed, and you have an IBM Cognos 8 gateway installed on a UNIX computer, you can set up the UNIX gateway for IBM Cognos 8 Planning. To do this, you must manually copy

some files from the Windows installation source files to your UNIX gateway computer. For more information, see "[Configure an IBM Cognos 8 UNIX Gateway for IBM Cognos 8 Planning](#)" (p. 138).

Steps

1. If you are installing to a directory with other IBM Cognos 8 components, stop the IBM Cognos 8 service.
2. Insert the IBM Cognos 8 Planning Server CD or go to the installation source file directory.
The **Welcome** page of the installation wizard appears when you insert the CD.
If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click issetup.exe.
3. Select the language to use for the installation.
The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.
4. In the **Component Selection** screen, select **Planning Gateway**.
If you are installing it in a directory that contains other IBM Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.
5. In the **Finish** page of the installation wizard,
 - If you want to configure Content Manager immediately, click **Start IBM Cognos Configuration**.
 - If you want to see late-breaking information about IBM Cognos components, click **View the Readme**.
6. Click **Finish**.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos 8 components and to start and stop IBM Cognos services.

Step

- From the **Start** menu, click **Programs, IBM Cognos 8, IBM Cognos Configuration**.

Configure Environment Properties for the Gateway

The gateway computer must know the location of at least one Planning Server dispatcher in your environment. The load management of Planning Server dispatchers is controlled by the Content Manager, which knows the location of all Planning Server dispatchers. Additional dispatchers that you configure on the gateway computer are used for failover purposes.

Steps

1. In the IBM Cognos Configuration **Explorer** window, click **Environment**.

2. In the **Properties** window, click the value for **Dispatcher URIs for gateway** and then click the edit button.
3. Edit the default value for a Planning Server dispatcher in your environment.
4. If you have installed more than one Planning Server, you can specify the URIs for the additional Planning Server dispatchers:
 - In the **Value - Dispatcher URIs for gateway** dialog box, click **Add**.
 - In the blank row of the table, click and then type the full URI of the Planning Server dispatcher.
 - Repeat the previous two bulleted steps for each additional URI.
 - Click **OK**.
5. In the **Explorer** window, under **Security, Cryptography**, click **IBM Cognos**, the default cryptographic provider.
6. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
7. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
8. From the **File** menu, click **Save**.

Configure the Web Server

You must create virtual directories to connect to the IBM Cognos 8 portal and for client applications to be able to connect to the server.

Step

- Create the following virtual directories:

Alias	Location	Permission
cognos8	<i>c8_location/webcontent</i>	Read
cognos8/cgi-bin	<i>c8_location/cgi-bin</i>	Execute

Note: The cogrcp folder, located in *c8_location/planning/contributor* must have **Scripts only** execute permissions.

You can use a name other than cognos8 in the aliases. However, you must use cgi-bin as the second part of the alias. If you use an alias other than cognos8 you must change the virtual directory in the **Gateway URI** property to match your alias.

For Apache Web Server, ensure that you define the cognos8/cgi-bin alias before the cognos8 alias in the httpd.conf file located in the *Apache_installation/conf* directory. You must define the cognos8/cgi-bin alias as a ScriptAlias.

Test the Gateway

You can test the installation using a Web browser.

Steps

1. Ensure that your Web server is running.
2. Open a Web browser.
3. In your address box, type the URI for the gateway. For example

`http://hostname/cognos8`

The IBM Cognos Connection **Welcome** page appears.

Uninstalling IBM Cognos 8 Planning

It is important to use uninstall programs to completely remove all files and modifications to system files.

Uninstall IBM Cognos 8 on Windows

If you no longer require IBM Cognos 8 or if you are upgrading, uninstall all IBM Cognos 8 components and the IBM Cognos 8 service.

If you installed more than one component in the same location, the uninstall wizard lets you choose the packages to uninstall. All components of the package will be uninstalled. You must repeat the uninstallation process on each computer that contains IBM Cognos 8 components.

It is not necessary to back up the configuration and data files on Windows. These files are preserved during the uninstallation.

We recommend that you close all programs before you uninstall IBM Cognos 8. Otherwise, some files may not be removed.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them using Windows Explorer.

Important: Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos 8 and you want to use the configuration data with the new version.

Steps

1. From the **Start** menu, click **Programs, IBM Cognos 8, Uninstall IBM Cognos 8**.

The **Uninstall** wizard appears.

Tip: IBM Cognos 8 is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.

2. Follow the instructions to uninstall the components.

The `cognos_uninst_log.htm` file records the activities that the Uninstall wizard performs while uninstalling files.

Tip: To find the log file, look in the Temp directory.

3. Delete all temporary Internet files.

For more information, see your Web browser documentation.

Chapter 8: Installing the Planning Clients

You can install the following IBM Cognos 8 Planning clients:

- ❑ [the administration components](#), including Analyst and Contributor Administration
- ❑ [Contributor Web Client](#)
- ❑ [Contributor for Microsoft Excel](#)
- ❑ [Framework Manager](#)
- ❑ [an Analyst network connection point](#)

Install IBM Cognos 8 Planning Administration Components

Install IBM Cognos 8 Planning administration components to have access to all IBM Cognos 8 Planning administration tools. You can select the administration components that you want to install and the location on your computer where you want to install them.

You can install

- Analyst
- *Analyst for Microsoft Excel*
- IBM Cognos Planning Manager
- Contributor Administration Console

Steps

1. Insert the CD for IBM Cognos 8 Planning Administration or go to the installation source file directory.

The **Welcome** page of the installation wizard should appear when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click `issetup.exe`.

2. Select the language to use for the installation.
3. Follow the directions in the installation wizard to copy the required files to your computer.

If an older version of the Microsoft Windows Installer Tool is installed on your computer, you are prompted to manually install Microsoft SOAP Toolkit before you configure your IBM Cognos 8 Planning environment.

If you are installing in a directory that already has other IBM Cognos 8 Planning components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

- Expand **Planning Administration**, and select the components that you want to install.

Tip: If you are installing *Analyst for Microsoft Excel* in a Citrix environment, you can select **Analyst for Microsoft Excel**, and select **To be run in a Citrix environment**.

- Choose how to proceed in the **Finish** page of the installation wizard:
 - If you want to configure IBM Cognos components immediately, click **Start IBM Cognos Configuration**.
 - If you want to see late-breaking information about IBM Cognos 8 Planning components, click **View the Readme**.
- Click **Finish**.

After you install administration components, you must configure the location of the IBM Cognos 8 Planning gateway and an IBM Cognos 8 Planning server.

Default Settings for IBM Cognos 8 Planning - Administration Components

The following table lists the default workspace size used by Analyst. After installation, you can use IBM Cognos Configuration to change this setting. You can also change it by editing the `cogstartup.xml` file in the `c8_location\configuration` directory.

Component	Default	Description
Analyst maximum workspace size in KB	64000	The amount of memory that the APL interpreter can use.

Configure Environment Properties for the Administration Components

The IBM Cognos 8 Planning administration components require the gateway URI and the URI of at least one Planning Server dispatcher in your environment.

Steps

- In the IBM Cognos Configuration **Explorer** window, click **Environment**.
- Type the value for the **Gateway URI**.
- Type the value for the **Dispatcher URI for external applications**.
The host name can be any Planning Server dispatcher in your environment (p. 91). Ensure that you use the server name or IP address, and the correct port number.
- In the **Explorer** window, under **Cryptography**, click **IBM Cognos**, the default cryptographic provider.
- Under the **Certificate Authority settings** property group, for the **Password** property, enter the same password you configured on the default active Content Manager computer.
- Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.

7. From the **File** menu, click **Save**.

Configuring Analyst Computers

When you install IBM Cognos 8 Planning - Server, Analyst is always installed even though it is not a selectable component. You can also install Analyst as an optional component when you install Analyst IBM Cognos 8 Planning - Administration.

Some configuration tasks are optional. You perform them to change the default property values used by Analyst.

Many Analyst configuration tasks are performed in Analyst. For more information, see the *Analyst User Guide*.

If you install Analyst on the same computer as other IBM Cognos 8 Planning components, no configuration is required if you

- configure your Web server using the default virtual directories
- use the default ports
- use the default resources
- use the default cryptographic settings

Configure Environment Properties for Analyst Computers

If you install Analyst on a computer than other IBM Cognos 8 Planning components, you must configure it to communicate with the other components.

You must also set up the planning data sources ([p. 44](#)) before you configure Analyst.

Important: If IBM Cognos 8 Planning was installed in more than one location, ensure that all URIs point to the correct version of IBM Cognos 8 Planning. Configure Analyst to use the same version of IBM Cognos 8 Planning.

Installations with a Firewall

When Analyst is outside a network firewall that protects the planning server components, communication issues with the dispatcher can arise. To avoid communication issues, you can install Analyst in the same architectural tier as the Planning Server components, or you can install and configure a gateway that is dedicated to Analyst communications.

Steps

1. On the computer where you installed Analyst, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Gateway URI** box, type the syntax that corresponds to the type of gateway you are using. Use the following table to find the syntax for your gateway:

Gateway Type	Syntax
ISAPI	Replace cognos.cgi with cognosisapi.dll
Apache Web server Module 1.3	http://host_name:port/cognos8/cgi-bin/mod_cognos.dll
Apache Web server Module 2.0	http://host_name:port/cognos8/cgi-bin/mod2_cognos.dll
Apache Web server Module 2.2.x	http://host_name:port/cognos8/cgi-bin/mod2_2_cognos.dll
Servlet gateway	http[s]://host_name:port/context_root/servlet/Gateway where <i>context_root</i> is the value you assigned to the ServletGateway Web application when you deployed the ServletGateway application.
Dispatcher	http[s]://host_name:port/p2pd/servlet/dispatch

Note: If you are using Apache Web Server for the Gateway URI, ensure that you configured it first.

4. Change the host name portion of the **Gateway URI** from localhost to either the IP address of the computer or the computer name.
5. In the **Explorer** window, under **Cryptography**, click **IBM Cognos**, the default cryptographic provider.
6. Under the **Certificate Authority settings** property group, for the **Password** property, enter the same password you configured on the default active Content Manager computer.
7. From the **File** menu, click **Save**.

Configure Integrated Windows Authentication

If you intend to run the Analyst Batch Scheduler wizard, you must configure integrated Windows authentication to secure jobs and macros in Analyst.

To use Integrated Windows Authentication, you must use an authentication provider that supports it. You can configure all authentication providers supported by IBM Cognos 8 to use Integrated Windows authentication, except for the SAP provider.

Steps

1. In Internet Information Services (IIS) Manager, right-click the virtual directory for Planning, and select **Properties**.

2. Click the **Directory Security** tab, and click **Edit** next to **Enable anonymous access and edit the authentication methods for this resource**.
3. Clear **Anonymous access**, and select **Integrated Windows authentication**. Click **OK**, and close IIS.

Change the Language of the Analyst Samples

The Analyst samples require no further setup if you want to access the samples in the language that you selected when you installed IBM Cognos 8 Planning server or administration components.

The `filesys.ini` file determines the language of the samples. To change languages, you must edit the `filesys.ini`.

The location of the Analyst samples depends on the type of installation you selected.

- If you created a network installation point, the samples are located on the computer with the network installation point, in the `\\server\shared_directory\samples\Planning\Analyst` folder.
- If you installed Analyst but did not create a network installation point, the samples are located locally on your computer in the `c8planning_location\samples\Planning\Analyst` folder.

Steps if You Created a Network Installation Point

1. In the `c8_location\uninstall` folder, open a command prompt.
2. Type the following:

```
uninst.exe -wct "\\server\
share\bin\wct\epAnalystFileSysCfg_
lang.xml"
```

where

- `\\server\share` is the location of the network installation point.
- `lang` is the language.

If `lang` is `de`, `filesys.ini` will point to the German samples.

If `lang` is `en`, `filesys.ini` will point to the English samples.

If `lang` is `fr`, `filesys.ini` will point to the French samples.

If `lang` is `sv`, `filesys.ini` will point to the Swedish samples.

Steps If Analyst was Installed Locally

1. In the `c8_location\uninstall` folder, open a command prompt.
2. Type the following:

```
uninst.exe -wct "\\c8_location\bin\wct\epAnalystFileSysCfg_lang.xml"
```

where

- `c8_location` is the location of the IBM Cognos 8 Planning installation on your computer.
- `lang` is the language.

If `lang` is `de`, `filesys.ini` will point to the German samples.

If *lang* is en, filesys.ini will point to the English samples.

If *lang* is fr, filesys.ini will point to the French samples.

If *lang* is sv, filesys.ini will point to the Swedish samples.

Contributor Web Client

Administrators can install one of following Web clients:

- [Contributor Web Client](#).
- [Classic Contributor Web client](#).

This is the original Web client.

Installation Options for the Contributor Web Client

An administrator or Contributor users can install this Web client.

- An administrator can install the Contributor Web Client for a single user or all users. This is done by [using a command line to install](#) the IBM Cognos 8 Planning 8.4 Client Framework and the IBM Cognos 8 Contributor 8.4.

Administrators can also install this client from the [IBM Cognos 8 Planning Client installation CD](#).

- A Contributor user can install the Web client by [clicking a Web link](#) on their Workflow page.

Installation Options for the Classic Contributor Web Client

Administrators can install the Classic client from the [IBM Cognos 8 Planning Client installation CD](#), or by [clicking a Web link](#).

Installing and Configuring the Web Client

Administrators use the Contributor Administration Console to set options for downloading, installing, and updating the Contributor Web Client.

Depending on the options the administrator sets, an administrator or a Contributor user can install the Web Client.

Installing and configuring the Contributor Web Client comprises the following tasks:

- ☐ [Set installation options using the Contributor Administration Console](#).
- ☐ [Install the Web Client using a Web link](#).
- ☐ [Install the Web Client using a command line](#).
- ☐ [Install the Web Client using the Planning Client installation CD](#).

Contributor users can uninstall the Contributor Web Client using the **Add or Remove Programs** on the Windows **Control Panel**.

The Contributor Administration Console must be installed before you can install and configure the Contributor Web Client ([p. 101](#)).

Set Installation Options the Contributor Web Client

Administrators set installation options using the Contributor Administration Console.

These installation options determine whether the administrator or the Contributor user installs the client. The settings also determine whether the updates are automatically received or if the administrator remotely installs the updates.

Note: These installation options apply to the Contributor and Classic Contributor clients. To use the Classic Web Client, you must select the **Use the classic Contributor client** check box on the **Go to Production Options** page.

Steps

1. On the **Contributor Administration Console**, select **System Settings**, and then click the **Web Client Settings** tab.
2. Do one of the following:
 - Select the **Allow automatic downloads and installations** check box to allow Contributor users to download and install the Web client from the Workflow page.
 - Clear **Allow automatic downloads and installations** check box to allow administrators to remotely install the MSIs using a command line installation, or CD.
3. Do one of the following:
 - Select **Allow automatic client software updates** check box to allow Contributor users to automatically receive Web client updates.
 - Clear **Allow automatic client software updates** check box to allow administrators to remotely install updates using the command line.

Note: If you clear the **Allow automatic downloads and installations** check box, Contributor users cannot install the Contributor Web Client. This means that an administrator must install the Contributor Web Client using a command line installation.

Install the Contributor Web Client Using a Web Link

If the **Allow automatic downloads and installations** is selected in the Contributor Administration Console, then Contributor users can download and install the Contributor Web Client on their machine.

Note: Contributor users only receive Contributor Web Client documentation after the client is installed. For this reason, we recommend that administrators provide installation and uninstallation instructions to Contributor users.

Steps

1. Log on to IBM Cognos Connection.

2. In IBM Cognos Connection, in the upper-right corner, click **Launch, Contributor**. If you have access to more than one package, click the package that you require.

On the workflow page, you see a graphical overview of all the areas you are responsible for, and the status of the data.

3. Click an eList item.

A new Contributor page appears, and you are prompted to install IBM Cognos 8 Planning 8.4 Client Framework.

4. Click **Install Now**.

5. On the **File Download** dialog box, click **Run** to install CognosRCP.msi.

6. Restart your Web browser.

IBM Cognos 8 Contributor 8.4 is now installed on the IBM Cognos 8 Planning 8.4 Client Framework. The Contributor Web Client opens the next time you navigate to a node on the workflow page.

Install the Contributor Web Client Using a Command Line

Administrators can install Contributor Web Client using a Windows Installer command line. This allows the client to be distributed using Active Directory or other software management tools.

Administrators use the command line to install the

- CognosRCP.msi.

This installs IBM Cognos 8 Planning 8.4 Client Framework.

- contributor.msi.

This installs IBM Cognos 8 Contributor 8.4. This installation does not require any command-line parameters. The location of the installed files are relative to the installation location of the IBM Cognos 8 Planning 8.4 Client Framework.

The commands that administrators can use to install CognosRCP.msi are described in the following table.

Command	Description
ALLUSERS=2	<p>Installs the MSI for all Contributor users.</p> <p>This command ensures that the registry entries for the IBM Cognos 8 Planning 8.4 Client Framework are located in HKEY_LOCAL_MACHINE.</p> <p>Note: You must use this command with the TARGETDIR command.</p>
TARGETDIR=" <i>CognosRCP_install_location</i> "	<p>Specifies the install location for the MSI. For example, TARGETDIR="C:\Program Files"</p>

Command	Description
NOUPDATE=Yes	Prevents Contributor users from receiving automatic updates for the IBM Cognos 8 Planning 8.4 Client Framework.

Steps to install the IBM Cognos 8 Planning Client Framework

1. Open a command prompt, and navigate to the location of the CognosRCP.msi file.

By default, the MSI files are located in *c8_location\webcontent\rcp_installs*

2. Install CognosRCP.msi by doing one of the following:

- To install the MSI for a single user, type the following command

```
CognosRCP.msi TARGETDIR="install_location"
```

Note: To prevent automatic updates for Contributor users add NOUPDATE=Yes before you execute the command.

- To install the MSI for all users, type the following command

```
CognosRCP.msi TARGETDIR="install_location" ALLUSERS=2
```

Note: To prevent automatic updates for Contributor users add NOUPDATE=Yes before you execute the command.

After you install the CognosRCP.msi, IBM Cognos 8 Planning 8.4 Client Framework appears on the Windows **Add or Remove Programs** list. In addition, a folder called CognosRCP is created in the installation location that you specified in the TARGETDIR command.

Steps to install IBM Cognos 8 Contributor

1. Open a command prompt, and navigate to the location of the contributor.msi file.

By default, the MSI files are located in *c8_location\webcontent\rcp_installs*

2. Type the following command:

```
contributor.msi
```

After the is successfully installed, IBM Cognos 8 Contributor 8.4 appears on the Windows **Add or Remove Programs** list.

Install the Web Client from the Planning Client Installation CD

Use the IBM Cognos 8 Planning Client installation CD to install Contributor or Classic Contributor as a Web Client or to use while you are offline.

If you are installing on Windows Vista and User Account Control (UAC) is enabled, you must start the installation wizard using **Run As Administrator**.

Steps

1. Insert the CD for IBM Cognos 8 Planning Client or go to the installation source file directory.

The **Welcome** page of the installation wizard should appear when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click `issetup.exe`.

If you are using Windows Vista and UAC is enabled, right-click `issetup.exe`, and select **Run As Administrator**.

2. Select the language to use for the installation.
3. Follow the directions in the installation wizard to copy the required files to your computer.

If you are installing in a directory that already has other IBM Cognos 8 Planning components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

4. Click **Finish**.

After you install the client, you can access the IBM Cognos 8 Planning portal to use Contributor Web.

The Classic Contributor Web Client does not require any configuration.

Uninstall the Contributor Web Client

The steps to uninstall the Contributor Web Client depend on how the client was installed.

If a Contributor user installed Contributor by clicking a Web link on the workflow page, then only the IBM Cognos 8 Planning 8.4 Client Framework appears on the **Add or Remove Programs** list. IBM Cognos 8 Contributor 8.4 appears in this list if an Administrator used the command line to install it.

Use **Add or Remove Programs** on the Windows **Control Panel** to uninstall the IBM Cognos 8 Planning 8.4 Client Framework or IBM Cognos 8 Contributor 8.4.

Note: To uninstall the Classic Contributor Web Client, see ["Uninstall IBM Cognos 8" \(p. 117\)](#).

Install Contributor *for Microsoft Excel*

Install Contributor *for Microsoft Excel* to view and edit Contributor data using Microsoft Excel formatting and linking functionality.

Do not install Contributor *for Microsoft Excel* on a computer that already has Analyst or Contributor Administration installed on it.

If you are installing on Windows Vista and User Account Control (UAC) is enabled, you must start the installation wizard using **Run As Administrator**.

If you are installing Contributor *for Microsoft Excel* on multiple computers, ensure that you install the same version on each computer.

If you have an older version of Contributor *for Microsoft Excel*, we recommend that you uninstall it before you install the IBM Cognos 8 version. Uninstalling does not remove any XLS worksheets that you have saved.

Steps

1. Insert the CD for IBM Cognos 8 Planning Client or go to the installation source file directory.

The **Welcome** page of the installation wizard should appear when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click `issetup.exe`.

If you are using Windows Vista and UAC is enabled, right-click `issetup.exe`, and select **Run As Administrator**.

2. Select the language to use for the installation.
3. Follow the directions in the installation wizard to copy the required files to your computer.

If you are installing in a directory that already has other IBM Cognos 8 Planning components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

4. Click **Finish**.

After you install the Client, you can access the IBM Cognos 8 Planning portal to use Contributor Web. The Contributor Web Client does not require any configuration.

When you start Microsoft Excel, **Contributor** appears in the Microsoft Excel menu bar. For more information about using Contributor *for Microsoft Excel*, see the IBM Cognos Planning - Contributor *for Microsoft Excel User Guide*.

Install Framework Manager

You can install Framework Manager, the metadata modeling tool for IBM Cognos 8, to create models from published planning packages. You can use the packages in IBM Cognos 8 studios. For example, you can create email notifications for milestones in your planning processes in Event Studio using a Framework Manager package.

Before you install Framework Manager, we recommend that you close all running programs to ensure that the installation program copies all the required files to your computer.

Also, ensure that you have administrator privileges for the computer on which you are installing. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer. Administrator privileges are also required for the account that runs Framework Manager.

We recommend that you install and configure all IBM Cognos 8 Planning server components before you install Framework Manager.

System Requirements for Framework Manager

Before you install Framework Manager, ensure that the Windows computer meets IBM Cognos 8 software and hardware requirements. The size of your models determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run Framework Manager.

Requirement	Specification
Operating system	Windows
RAM	Minimum: 512 MB Recommended: 1 GB
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory used by IBM Cognos 8
Database	Database client software installed on the same computer as Framework Manager (Oracle, DB2, or Sybase only) Database connectivity set up
Other	Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples

Steps

1. If you use an Oracle database as a data source for your reports, set the NLS_LANG environment variable by typing the following command on each computer where Framework Manager or a Planning Server is installed:

NLS_LANG = language_territory.character_set

For example, NLS_LANG = JAPANESE_JAPAN.UTF8

The value of the variable determines the locale-dependent behavior of IBM Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

2. If you are installing in a directory with other IBM Cognos 8 components, stop the IBM Cognos 8 service.
3. Insert the IBM Cognos 8 Business Intelligence Modeling CD or go to the installation source file directory.

The **Welcome** page of the installation wizard appears when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click issetup.exe.

4. Select the language to use for the installation.

The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

5. Follow the directions in the installation wizard to copy the required files to your computer.

Install IBM Cognos 8 components in a directory that contains only ASCII characters in the path name. Some Windows Web servers do not support non-ASCII characters in directory names.

If you are installing IBM Cognos 8 on a computer that already has ReportNet, and you want to keep ReportNet running, you must install IBM Cognos 8 in a different directory.

If you are installing in a directory that contains other IBM Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

6. In the **Finish** page of the installation wizard,
 - If you want to configure IBM Cognos components immediately, click **Start IBM Cognos Configuration**.
 - If you want to see late-breaking information about IBM Cognos components, click **View the IBM Cognos Readme**.

7. Click **Finish**.

Use the Windows **Start** menu to start **IBM Cognos Configuration** from the shortcut folder.

To ensure the security and integrity of IBM Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

If you use Oracle, DB2, or Sybase as the database server for the content store in a distributed installation, you must now install the database client software ([p. 49](#)) on the same computer where you installed Framework Manager.

Default Settings for Framework Manager

The following table lists the default settings for the IBM Cognos 8 ports and URIs that Framework Manager uses. After installation, you can use the configuration tool to change the settings. You can also change them by editing the `cogstartup.xml` file in the `c8_location\configuration` directory.

Component	Default	Description
Gateway	<code>http://localhost:80/cognos8/cgi-bin/cognos.cgi</code>	The URI to the IBM Cognos 8 gateway
Dispatcher URI for external applications	<code>http://localhost:9300/p2pd/servlet/dispatch</code>	The URI to the dispatcher
Log Server Port	9362	The port used by the local log server

Configure Environment Properties for Framework Manager Computers

If you install Framework Manager on a different computer from the non-modeling components of IBM Cognos 8, you must configure it to communicate with the other components.

We recommend that you install and configure IBM Cognos 8 components before you configure Framework Manager. You must first install and configure Content Manager and then start the IBM Cognos 8 service on at least one Content Manager computer before you configure Framework Manager. This ensures that the certificate authority service issues a certificate to the Framework Manager computer.

Important: If IBM Cognos 8 was installed in more than one location, ensure that all URIs point to the correct version of IBM Cognos 8. Framework Manager must be configured to use the same version of IBM Cognos 8.

Installations with a Firewall

When the modeling tool is outside a network firewall that protects the Planning Server components, communication issues with the dispatcher can arise. To avoid communication issues, you can install the modeling tool in the same architectural tier as the Planning Server components or you can install and configure a gateway that is dedicated to modeling tool communications.

Prerequisites

You must also set up the data sources ([p. 52](#)) before you configure Framework Manager.

Steps

1. On the computer where you installed Framework Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Gateway URI** box, type the syntax that corresponds to the type of gateway you are using. Use the following table to find the syntax for your gateway:

Gateway Type	Syntax
ISAPI	Replace cognos.cgi with cognosisapi.dll
Apache Web server Module 1.3	http://host_name:port/cognos8/cgi-bin/mod_cognos.dll
Apache Web server Module 2.0	http://host_name:port/cognos8/cgi-bin/mod2_cognos.dll
Apache Web server Module 2.2.x	http://host_name:port/cognos8/cgi-bin/mod2_2_cognos.dll

Gateway Type	Syntax
Servlet gateway	<code>http[s]://host_name:port/context_root/servlet/Gateway</code> where <i>context_root</i> is the value you assigned to the ServletGateway Web application when you deployed the ServletGateway application.
Dispatcher	<code>http[s]://host_name:port/p2pd/servlet/dispatch</code>

Note: If you are using Apache Web Server for the Gateway URI, ensure that you configured it first.

4. Change the host name portion of the **Gateway URI** from `localhost` to either the IP address of the computer or the computer name.
5. Specify the value for the **Dispatcher URI for external applications**.
 - If your Web server is configured not to allow anonymous access, type the URI of the dispatcher, ensuring that you change the host name in the URI from `localhost`.
 - If your Web server supports chunked transfer encoding and Framework Manager is inside the firewall, type the URI of the dispatcher, ensuring that you change the host name in the URI from `localhost`.
 - If you are using a dedicated gateway for modeling tool communication, type the dispatcher URI.
6. In the **Explorer** window, under **Cryptography**, click **IBM Cognos**, the default cryptographic provider.
7. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password you configured on the default active Content Manager computer.
8. From the **File** menu, click **Save**.

Framework Manager is configured to communicate with the other components of IBM Cognos 8. You can [configure a source control system](#).

Configure a Source Control System

To help you manage, share, and secure different versions of your metadata, you can configure Framework Manager to use a source control system.

You must already have one of the following source control system clients set up on the same computer as Framework Manager:

- Component Software Concurrent Versions System
- Visual Source Safe

For more information about installing and setting up source control systems, see Repository Control in the Framework Manager *User Guide*.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, right-click **Source Control Systems** and click **New resource, Source Control System**.
Source Control System is available on computers that have Framework Manager installed.
3. In the **Name** box, type a name for your source control system.
4. In the **Type** box, select a source control system from the list.
5. Click **OK**.
6. In the **Properties** window, for the **Source control system executable file (.exe) location** property, specify the file location and name of the .exe file.
 - For VSS, type `file_location\ss.exe`
 - For CVS, type `file_location\cvs-version.exe`
where *version* is the CVS version number.
7. From the **File** menu, click **Save**.

Install an Analyst Network Connection Point

A network connection point is the location where you set up a network share. For distributed Analyst installations, you should always install a network connection point so that both Analyst server and Analyst clients use a Universal Naming Convention (UNC) path to connect to a shared library.

When you create a network connection point, the Analyst software is installed on the local drive of your computer, and the data is stored in a shared location on the network server, along with control files and the samples files.

One of the files created at the network installation point is `filesys.ini`. The `filesys.ini` file is a control file used by Analyst. It contains file paths for the `Libs.tab`, `Users.tab`, and `Groups.tab` that control the specific library and user setup. If you do not specify the `filesys.ini` path by creating a network connection point, you must specify the path when you create planning tables. For more information, see the Contributor *Administration Guide* or the Analyst *User Guide*.

Before you begin the installation, you must set up a network share so that server and client computers can access the installation files. Ensure that all Analyst users have NTFS permissions of Modify.

Steps

1. Insert the CD for IBM Cognos 8 Planning Server or go to the installation source file directory.
The **Welcome** page of the installation wizard appears when you insert the CD.

If no **Welcome** page appears or you are not installing from the CD, go to the win32 directory, and double-click issetup.exe.

If you are using Windows Vista and UAC is enabled, right-click issetup.exe, and select **Run As Administrator**.

2. Select the language to use for the installation.

The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

3. In the **Component Selection** screen, select **Analyst UNC Connection Point**, and clear all other components.
4. In the **Analyst UNC Install Location** screen, type the UNC path for the shared directory to which you want the network installation point installed.
5. In the **Finish** page of the installation wizard,
 - If you want to configure Content Manager immediately, click **Start IBM Cognos Configuration**.
 - If you want to see late-breaking information about IBM Cognos components, click **View the Readme**.
6. Click **Finish**.

Uninstall IBM Cognos 8

It is important to use uninstall programs to completely remove all files and modifications to system files.

If you no longer require IBM Cognos 8 or if you are upgrading, uninstall all IBM Cognos 8 components and the IBM Cognos 8 service.

If you installed more than one component in the same location, the uninstall wizard lets you choose the packages to uninstall. All components of the package will be uninstalled. You must repeat the uninstallation process on each computer that contains IBM Cognos 8 components.

It is not necessary to back up the configuration and data files on Windows. These files are preserved during the uninstallation.

We recommend that you close all programs before you uninstall IBM Cognos 8. Otherwise, some files may not be removed.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them using Windows Explorer.

Important: Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos 8 and you want to use the configuration data with the new version.

Steps

1. From the **Start** menu, click **Programs, IBM Cognos 8, Uninstall IBM Cognos 8**.

The **Uninstall** wizard appears.

Tip: IBM Cognos 8 is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.

2. Follow the instructions to uninstall the components.

The cognos_uninst_log.htm file records the activities that the Uninstall wizard performs while uninstalling files.

Tip: To find the log file, look in the Temp directory.

3. Delete all temporary Internet files.

For more information, see your Web browser documentation.

Chapter 9: Additional Configuration Options

After you install one or more IBM Cognos 8 Planning components on your computer, you must configure them to work in your IBM Cognos environment. Initially, default property settings are used to configure the components. However, you may want to change these default settings if existing conditions make the default choices inappropriate, or to better suit your environment.

Other configuration tasks are optional and depend on your IBM Cognos environment. Use these optional configuration tasks to customize your configuration so that IBM Cognos 8 Planning easily integrates into your existing environment. For example, you can configure features for IBM Cognos Application Firewall or specify the amount of resources IBM Cognos 8 uses. Also, you can deliver IBM Cognos content using any other portal by configuring Portal Services.

You can configure IBM Cognos 8 Planning to use other resources, such as using an authentication provider and then enabling single signon for the database connection and the users.

If you use a load-balancing scheme in your environment, you can change settings to improve performance. For example, you can balance requests among dispatchers by changing their processing capacity or by setting the minimum and maximum number of processes and connections. For more information about tuning server performance, see the *Administration and Security Guide*.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos 8 components and to start and stop IBM Cognos services.

Step

- From the **Start** menu, click **Programs, IBM Cognos 8, IBM Cognos Configuration**.

Changing Default Configuration Settings

When you install IBM Cognos 8 components, the installation uses default configuration settings. If you have any reason not to use these default values, such as a port is being used by another process, use IBM Cognos Configuration to change the value.

If you change the value of a property, you must save the configuration and then restart the IBM Cognos 8 service to apply the new settings to your computer.

For distributed installations, ensure that you configured all computers where you installed Content Manager before you change default configuration settings on other IBM Cognos computers. For example you can

- [change a URI](#)
- [configure cryptographic settings](#)
- [configure IBM Cognos 8 components to use IBM Cognos Application Firewall](#)

- [configure the gateway to use a namespace](#)
- [enable and disable services](#)
- [specify the amount of resources the IBM Cognos 8 service uses](#)

Change a URI

You can change certain elements in a URI depending on your environment. A IBM Cognos URI contains the following elements:

- For a Content Manager URI, Dispatcher URI for external applications, or dispatcher URI
protocol://host_name_or_IP:port/context_root/alias_path
- For a Gateway URI or a Web content URI
protocol://host_name_or_IP:port/virtual_directory/gateway_application
OR
protocol://host_name_or_IP:port/context_root/alias_path

Element	Examples	Description
protocol	http or https	Specifies the protocol used to request and transmit information, either Hyper Text Transfer Protocol or Hyper Text Transfer Protocol (Secure).
host name or IP	localhost or 192.168.0.1 or [2001:0db8:0000:0000:0000:0000:148:57ab]:80	Specifies the identity of the host on the network. You can use an IP address, a computer name, or a fully qualified domain name. In a distributed installation, you must change the localhost element of a URI.
port	9300 or 80	Specifies the port on which the host system listens for requests. The default port for Tomcat is 9300. The default port for a Web server is 80.

Element	Examples	Description
context root	p2pd	Used by Tomcat or an application server to determine the context of the application so that the request can be routed to the correct Web application for processing.
alias path	servlet/dispatch	Used by the application server to route a request to the correct component within a Web application. The alias path must not be modified or IBM Cognos 8 components will not function properly.
virtual directory	cognos8/	Used by the Web server to map a virtual directory or alias to a physical location. For example, in the default Gateway URI of http://localhost:80/cognos8/cgi-bin/cognos.cgi, the virtual directory is cognos8/cgi-bin.
gateway application	cognos.cgi	Specifies the name of the IBM Cognos gateway application that is used. For example, if you are accessing IBM Cognos 8 components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window click the appropriate group or component:
 - To change an element for the dispatcher, click **Environment**.
 - To change an element for the local log server, under **Environment**, click **Logging**.

3. In the **Properties** window, click the **Value** box next to the URI property that you want to change.
4. Select the element and type the new information.
Tip: To change the port used by the local dispatcher, change the value of the internal dispatcher URI property. Because the change affects all the URIs that are based on the local dispatcher, you must change the URIs of all local components.
Tip: If you change the dispatcher port in the dispatcher URI, ensure that you specify the new port number when you configure remote computers that use the dispatcher, Content Manager, or SDK services on this system.
5. From the **File** menu, click **Save**.

Configure Cryptographic Settings

IBM Cognos 8 components require a cryptographic provider; otherwise they will not run. If you delete the default cryptographic provider, you must configure another provider to replace it.

You can configure cryptographic provider settings, including the following:

- advanced algorithms
These include signing and digest algorithms.
- common symmetric key store (CSK) properties
The CSK is used by IBM Cognos 8 to encrypt and decrypt data.
- signing key store properties
The signing key pair includes the private key used to generate the digital signature and the public key used to verify authenticity.
- encryption key store properties
The encryption key pair includes the private key used to encrypt data and the public key used to decrypt data.

The default cryptographic provider uses keys up to 56 bits in length for data encryption and secure sockets layer (SSL) protocol. You can configure other cryptographic providers which use key sizes greater than 56 bits, such as the Enhanced Encryption Module for OpenSSL. For more information, see the *Enhanced Encryption Module for Entrust Installation and Configuration Guide*.

Important: In a distributed installation, IBM Cognos computers communicate with Content Manager to establish trust and obtain some cryptographic keys from Content Manager. If you change the cryptographic keys in Content Manager, such as by changing application servers or reinstalling Content Manager, you must delete the cryptographic keys on the other IBM Cognos computers. You must then save the configuration on each computer so that they obtain the new cryptographic keys from Content Manager. In addition, all IBM Cognos 8 components in a distributed installation must be configured with the same cryptographic provider settings.

Also, in a distributed environment, the symmetric key should only be stored on computers where Content Manager has been installed.

Steps for Cryptographic Settings

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, change the default values by clicking the **Value** box and then selecting the appropriate value:
 - On computers that do not contain Content Manager, if you do not want to store the CSKs locally, under **CSK settings**, change **Store symmetric key locally** to **False**.
When **Store symmetric key locally** is **False**, the key is retrieved from Content Manager when required. The **Common symmetric key store location** property is ignored.
 - If you want to change the digest algorithm, for the **Digest algorithm** property, select another value.
4. From the **File** menu, click **Save**.
5. Test the cryptographic provider on a gateway computer only. In the **Explorer** window, right-click **Cryptography** and click **Test**.

IBM Cognos 8 components check the availability of the symmetric key.

After you configure the cryptographic provider, passwords in your configuration and any data you create are encrypted.

Steps for Cryptographic Provider

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Cryptography**, click **IBM Cognos**.
 - If you want to change the location of the signing keys, under **Signing key settings**, change the **Signing key store location** property to the new location.
 - If you want to change the location of the encryption keys, under **Encryption key settings**, change **Encryption key store location** to the new location.
 - If you want to use another certificate authority, under **Certificate Authority settings**, change **Use third party CA** to **True**.

You must also ensure that you use the same values for the **-k** parameter as you used for the **Signing key store location** and **Encryption key store location** properties.

Important: The **Confidentiality algorithm** value determines how data is encrypted by IBM Cognos 8 components. For example, database passwords entered in IBM Cognos Configuration are encrypted when you save the configuration. The algorithm selected when the data is encrypted must also be available for the data to be decrypted at a later date.

The availability of confidentiality algorithms can change if there are changes to your environment. For example, if your Java Runtime Environment (JRE) has changed or if you have installed

other cryptographic software on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the availability of confidentiality algorithms. You must ensure that the **Confidentiality algorithm** that was selected when the data was encrypted is also available when you want to access the data.

3. From the **File** menu, click **Save**.

If you use another Certificate Authority (CA) server, you must now configure IBM Cognos 8 components to use the CA.

Configure IBM Cognos 8 Components to Use IBM Cognos Application Firewall

IBM Cognos Application Firewall analyzes and validates HTTP and XML requests before they are processed by IBM Cognos servers. IBM Cognos Application Firewall may modify these HTTP and XML requests.

IBM Cognos Application Firewall protects IBM Cognos Web products from malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting (XSS) attacks, either through script injection in valid pages or redirection to another Web site.

Using IBM Cognos Configuration, you can change settings for other XSS tool support, and you can add host and domain names to the IBM Cognos list of valid names.

You can track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the *c8_location\logs\cogserver.log* file.

Important: All CAF settings must be the same for all computers where IBM Cognos 8 Application Tier Components are installed within a distributed environment. For example, if CAF is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

The following types of URLs are accepted by CAF validation:

- fully qualified (absolute) URLs
in the format *protocol://host:port/path*, where *protocol* is http or https and *host* is validated against the valid domain list
- URLs relative to the Web installation directory
in the format */Web_installation_root/** where *Web_installation_root* is the gateway Web directory, based on the cognos8 alias that you configured on your Web server.
For more information, see (p. 98).
For example,
/cognos8/ps/portal/images/action_delete.gif
- specific allowed URLs, including the following (all case insensitive)
about:blank
JavaScript>window.close()
JavaScript:parent.close()
JavaScript:history.back()

```
parent.cancelErrorPage( )
doCancel( )
```

Steps

1. On each computer where an IBM Cognos 8 Planning Server has been installed, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **IBM Cognos Application Firewall**.
3. In the **Properties** window, for the **Enable CAF validation** property, set the appropriate values. By default, IBM Cognos Application Firewall is enabled.

Important: The IBM Cognos Application Firewall is an essential component of IBM Cognos security, helping to provide protection against penetration vulnerabilities. Disabling the IBM Cognos Application Firewall will remove this protection. Under normal circumstances we recommend that you not disable the IBM Cognos Application Firewall.

4. If you are using another XSS tool that checks for specific characters in GET request parameters, in the **Properties** window, do the following:
 - For the **Is third party XSS checking enabled** property, change the value to **True**.
 - For the **Third party XSS characters** property, add any additional characters that are prohibited by the other XSS tool. The default characters are >, <, and '.
5. Add host and domain names to the IBM Cognos list of valid names:
 - For the **Valid domains and hosts** property, click the value and then click the edit button.
 - In the **Value - Valid domains or hosts** dialog box, click **Add**.

You must include the domains from all hyperlinks that are added in IBM Cognos Connection. For more information, see the topic about creating a URL in the *Administration and Security Guide*.

Tip: If you are using drill-through from IBM Cognos Series 7 to reports in IBM Cognos 8, add the hostnames of the IBM Cognos Series 7 gateway servers to the list.

- In the blank row of the table, click and then type the host or domain name.
- Repeat the previous two bulleted steps for each name to be added.
- Click **OK**.

IBM Cognos Application Firewall validates domain and host names to protect URLs that are created. By default, IBM Cognos Application Firewall considers domain names derived from the environment configuration properties to be safe domain names. Adding names to the list of valid names and hosts is useful when you need to redirect requests to non-IBM Cognos computers using the Back or Cancel functions or when using drill-through to different IBM Cognos product installations.

6. Save the configuration.

7. Restart the services.

Configure the Gateway to Use a Namespace

If IBM Cognos 8 components use multiple namespaces or if anonymous access is enabled and IBM Cognos 8 components use one namespace, you can configure the gateway to connect to one namespace. Users logged onto the Web server where the gateway is located are not prompted to choose an authentication source.

For example, if you have two Web servers, you can configure each Web server to use a different namespace.

Steps

1. On the computer where the gateway is located, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Value** box next to the **Gateway namespace** property, type the Namespace ID of the namespace you want to use.
4. From the **File** menu, click **Save**.
5. Restart your Web server.

Enable and Disable Services

In a distributed installation, you can send certain types of requests to specific computers by enabling or disabling the installed services.

Note: The default values for dispatcher service and presentation service are false on computers that have the Content Manager only installed. On all other types of installations, the default values are true.

If you installed all components on several computers, you can disable appropriate services on each computer to get the distributed configuration you require. Requests are sent only to dispatchers where a given service is enabled.

Disabling a service prevents the service from loading into memory. When disabled, services do not start and therefore do not consume resources. The service does not run until you enable it.

If you disable the dispatcher service, all services that run under that dispatcher are also disabled. Only dispatcher services that are enabled can process requests.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **IBM Cognos 8 service**.
3. In the **Properties** window, click the **Value** next to the service that you want to disable or enable.
By default, all services are enabled.
4. Click the appropriate state for the services:

- To disable the service, click **False**.
- To enable the service, click **True**.

For example:

- for a Planning job server, you must enable the dispatcher service, the monitoring service, and the Planning job service. All other services can be disabled.
- for a Planning data server, you must enable the dispatcher service, the monitoring service, and the Planning data service.
- for a Planning administration server, you must enable the dispatcher service, the monitoring service, and the Planning administration console service.
- for a Planning Web server, you must enable the dispatcher service, the monitoring service, and the Planning Web service.

If you are configuring role-based Planning servers, you must also ensure that at least one Planning server has all the other IBM Cognos 8 services running.

5. From the **File** menu, click **Save**.

Specify Resources for the IBM Cognos 8 Service

To improve performance in a distributed environment, you can change the amount of resources that the IBM Cognos 8 service uses by choosing a configuration template.

By default, the IBM Cognos 8 service is configured to use minimal memory resources to optimize startup time.

The IBM Cognos 8 service is available only on the computers where you installed Content Manager or the Planning Server components.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, **IBM Cognos 8 service**, right-click **IBM Cognos 8**, and click **Delete**.

This deletes the default configuration template for the service.

3. Right-click **IBM Cognos 8 service**, and click **New resource, Configuration**.
4. Type a name for the service.

In Windows, the name you choose is used to register the service. You will see this name in the list of services running on your computer.

5. In the **Type** box, click the configuration template to use:
 - If you previously changed the default setting and now want to reduce the startup time, memory footprint, and resources used, click **Small configuration**.

- If you want a balance between fast startup time and quick operating speeds, click **Medium configuration**.
 - If you want to maximize operating speeds and if performance is more important than fast startup time, and if your computer has a lot of resources, click **Large configuration**.
6. In the **Properties** window, edit the properties so that they are appropriate for your environment.
 7. From the **File** menu, click **Save**.

Enable SSL on the Web Server

Enable secure sockets layer (SSL) to encrypt a user's communication with the Web server.

To enable SSL on your Web server, you must obtain a Web server certificate signed by a Certificate Authority (CA) and install it into your Web server. The certificate must not be self-signed, because self-signed certificates will not be trusted by IBM Cognos components.

To enable IBM Cognos components to use an SSL-enabled Web server, you must have copies of the trusted root certificate (the certificate of the root CA which signed the Web server certificate) and all other certificates which make up the chain of trust for the Web server's certificate. These certificates must be Base64 encoded in ASCII (PEM) or DER format. The certificates must be installed on every computer where you have installed Planning Server components.

For more information about installing certificates into your Web server, see your Web server documentation.

The Web server where SSL is enabled must have a valid certificate. If the certificate is not issued by a well known and trusted CA, such as a trial certificate or one issued by a private CA, then you must ensure that the corresponding root CA is installed on each computer that will access the portal. For example, in Internet Explorer, you can view the root authorities by clicking **Tools**, **Internet Options** and then clicking the **Content** tab, and the **Certificates** button. If the root authority for your certificate is not listed, you must import the certificate.

Steps

1. Configure the Web server for SSL and start the Web server.

For more information, see your Web server documentation

2. On each Planning Server computer that points to the gateway, in IBM Cognos Configuration, change the gateway URI from HTTP to HTTPS, and save the configuration.

Important: Do not start the IBM Cognos 8 service yet.

3. On each Planning Server computer, go to the `c8_location/bin` directory. Starting in order, with the root CA certificate, import the certificates (that make the chain of trust) to the IBM Cognos trust store.

Import the certificates by typing the following command:

```
ThirdPartyCertificateTool.bat -java:local -T -i -r certificate_fileName -D ../configuration/  
signkeypair -p NoPassWordSet
```


Note: The default password is NoPassWordSet.

4. On each Planning Server computer, in IBM Cognos Configuration, start the IBM Cognos 8 service.

To avoid being prompted by a security alert for each new session, install the certificate into one of your Web browser's certificate stores.

In addition, you may want to set up SSL connections between IBM Cognos components and other servers. You must ensure that SSL is set up for the other servers and then you must set up a shared trust between IBM Cognos components and the other servers.

Tip: For Apache Web server on UNIX, if you specified a fully qualified server name when you created the certificate, you must also specify a fully qualified server name in IBM Cognos Configuration when you specify the gateway URI.

Configuring the SSL Protocol

The Secure Sockets Layer (SSL) protocol is used to secure communication between IBM Cognos components installed on the same computer or on different computers.

In addition, you may want to set up SSL connections between IBM Cognos components and other servers. You must ensure that SSL is set up for the other servers and then you must set up a shared trust between IBM Cognos components and the other servers.

After configuring the SSL protocol, you can select and rank cipher suites, which control the quality of protection used in the SSL connection.

To configure SSL protocol, do the following:

- ❑ Configure SSL for IBM Cognos components ([p. 129](#)).
- ❑ Set up shared trust between IBM Cognos components and other servers, if required ([p. 132](#)).
- ❑ Select and rank Cipher Suites to be used in an SSL connection, if required ([p. 133](#)).
- ❑ Enable SSL on your Web server ([p. 133](#)).

Configure SSL for IBM Cognos 8

You can configure IBM Cognos components to use the SSL protocol for

- internal connections only
- external connections only
- internal and external connections
- connections to local and remote log servers

If you configure SSL only for internal connections, IBM Cognos components on the local computer communicate using this protocol. The dispatcher listens for secure connections on a different port than for remote, http requests. Therefore, you must configure two dispatcher URIs.

If you configure SSL only for external connections, communications from remote IBM Cognos components to the local computer use the SSL protocol. You must configure the dispatcher to listen for secure, remote requests on a different port than local, HTTP requests. You must also configure the Content Manager URIs and the dispatcher URI for external applications to use the same protocol and port as the external dispatcher.

If you configure SSL for all connections, the dispatcher can use the same port for internal and external connections. Similarly, if you do not use SSL for local or remote communication, the dispatcher can use the same port for all communications.

You must also update the Content Manager URIs, Dispatcher URI for external applications, and Gateway URI to use SSL, if required.

Tomcat Connectors

If the internal dispatcher URI is prefixed with http but the external dispatcher URI is prefixed with https, or vice versa, both the non-SSL Coyote HTTP/1.1 and SSL Coyote HTTP/1.1 connectors are enabled in the server.xml file.

If the internal and external dispatcher URIs use different protocol or ports, the internal dispatcher port is accessible only to the components on the local computer. The internal dispatcher URI must also specify localhost.

Single Computer Installations

In single computer installations, if you are running IBM Cognos 8 without SSL, you must stop the service before adding SSL to your configuration. After you save the configuration with SSL settings, you can restart the service.

Distributed Installations

In distributed installations, if you are using the IBM Cognos certificate authority service, you must first configure all IBM Cognos computers to use the non-secure (http) protocol before you configure IBM Cognos components to use the SSL protocol. You must do this because you cannot set up the SSL protocol before trust has been established.

Also, ensure that you follow the required order of configuring computers in a distributed environment. That means that you must first configure the computer where the default active Content Manager is installed and then start the services on this computer before you configure other computers or start services on other computers. By first configuring the default active Content Manager computer and starting the services, you ensure that the certificate authority service on the default active Content Manager computer can issue certificates to other computers in the IBM Cognos environment.

After you configure all computers in the distributed installation to use the default, non-secure protocol, we recommend that you test your installation to ensure that IBM Cognos components are working properly. After you test your installation, you can configure the SSL protocol.

When you configure IBM Cognos 8 to use the SSL protocol, ensure that you first configure the default active Content Manager computer to use the protocol and start the services on the default active Content Manager computer. After you do this, you can configure the SSL protocol on other IBM Cognos computers in your environment.

Add a Computer to an Installation

If you add a computer to an SSL-enabled environment, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the Content Manager computer.

Add a Component to a Computer

You can later add a component to the same location as other IBM Cognos components. If you add the component to a different location on the same computer as other IBM Cognos components, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established between the new component and the Content Manager computer.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, type the appropriate values for the **Internal dispatcher URI** and **External dispatcher URI** values:
 - To configure SSL for internal connections only, for the **Internal dispatcher URI** property, type **https** and a port for SSL communication. For the **External dispatcher URI** property, type **http** and use the default or another available port.
 If you use Tomcat, the **Internal dispatcher URI** property must also specify **localhost**.
 The ports in the two dispatcher URIs must be different.
 - To configure SSL for external connections only, for the **External dispatcher URI** property, type **https** and a secure port. For the **Internal dispatcher URI** property, type **http** and use the default or another available port.
 If you use Tomcat, the **Internal dispatcher URI** property must also specify **localhost**.
 The ports in the two dispatcher URIs must be different.
 - To configure SSL for all connections, type the same URI for both the **Internal dispatcher URI** and **External dispatcher URI** properties. Type **https** and a secure port, such as 9343.

Note: You do not have to use port 9343, the default SSL port. You can choose any available port.
4. Configure the SSL protocol for the other environment URIs, including the **Content Manager URIs**, the **Dispatcher URI for external applications**, and **Gateway URI**.
 - For internal connections only, type **https** in the URIs that contain **localhost**.
 - For external connections only, type **https** in the URIs that do not contain **localhost**.
 - For all connections, type **https** in all the URIs.
5. In the **Explorer** window, click **Security, Cryptography**.

6. To use SSL protocol, you must specify passwords for the IBM Cognos 8 encryption key stores. There are more settings under **Security, Cryptography, IBM Cognos**.
7. From the **File** menu, click **Save**.

Set Up Shared Trust Between IBM Cognos Servers and Other Servers

If you want to use the default IBM Cognos certificate authority and you want to use SSL for connections from other servers to IBM Cognos servers, you must add the IBM Cognos certificate to the trust store on the other servers.

Note: If you use browsers to connect to IBM Cognos components, the browsers automatically prompt users to update their trust stores.

If you want the connection between IBM Cognos servers and the other server to be mutually authenticated, you must also copy the certificate from your certificate authority to the trust store for IBM Cognos servers.

If you have configured IBM Cognos components to use another certificate authority (CA), you do not have to set up shared trust between IBM Cognos server and other servers.

Steps to Copy the IBM Cognos Certificate to Another Server

1. Go to the *c8_location\bin* directory.
2. Extract the IBM Cognos certificate by typing the following command:
 - On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -E -T -r destination_file -k c8_location/configuration/signkeypair/jCAKeystore -p password
```
 - On Windows, type

```
ThirdPartyCertificateTool.bat -E -T -r destination_file -k c8_location\configuration\signkeypair\jCAKeystore -p password
```
3. Import the certificate to the trust store on your server.
For information on updating the server trust store, see the documentation for your server.

Steps to Copy the CA Certificate to IBM Cognos Servers

1. Copy the certificate from your certificate authority to a secure location on the IBM Cognos server.
Ensure that the CA certificate is in Base-64 encoded X.509 format.
2. Import the CA certificate by typing the following command:
 - On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -T -i -r CA_certificate_file -k c8_location/configuration/signkeypair/jCAKeystore -p password
```
 - On Windows, type

```
ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -k c8_location\configuration\
signkeypair\jCAKeystore -p password
```

Select and Rank Cipher Suites for SSL

An SSL connection begins with a negotiation in which the client and server present a list of supported cipher suites in a priority sequence. A cipher suite provides the quality of protection for the connection. It contains cryptographic, authentication, hash, and key exchange algorithms. The SSL protocol selects the highest priority suite that the client and the server both support.

A list of supported cipher suites for SSL is provided. You can eliminate cipher suites that do not meet your requirements and then assign a priority, or preference, to the remaining cipher suites. The selected cipher suites are presented in priority sequence for the client and server sides of the negotiation. At least one of the selected cipher suites between the client and server platforms must match.

The list of supported cipher suites is dynamically generated on each computer, and depends on the Java Runtime Environment (JRE) or whether you have other cryptographic software installed on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the supported cipher suites available on that computer. If you no longer have a supported cipher suite that matches the other computers in your environment, you may have to change the JRE on the computer to match the other computers in your environment.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Cryptography, IBM Cognos**.
3. In the **Properties** window, click the **Value** column for the **Supported ciphersuites** property.
4. Click the edit button.
 - To move a cipher suite to the **Current values** list, click the check box in the **Available values** list and then click **Add**.
 - To move a cipher suite up or down in the **Current values** list, click the check box and then click the up or down arrows.
 - To remove a cipher suite from the **Current values** list, click the check box and then click **Remove**.
5. Click **OK**.
6. From the **File** menu, click **Save**.

Enable SSL on the Web Server

Enable secure sockets layer (SSL) to encrypt a user's communication with the Web server.

To enable SSL on your Web server, you must obtain a Web server certificate signed by a Certificate Authority and install it into your Web server. The certificate must not be self-signed, because self-signed certificates will not be trusted by IBM Cognos components.

To enable IBM Cognos components to use an SSL-enabled Web server, you must have copies of the trusted root certificate (the certificate of the root Certificate Authority which signed the Web server certificate) and all other certificates which make up the chain of trust for the Web server's certificate. These certificates must be in Base64 encoded in ASCII (PEM) or DER format, and must not be self-signed. The certificates must be installed on every computer where you have installed Planning Server components.

For more information about installing certificates into your Web server, see your Web server documentation.

Steps

1. Configure the Web server for SSL and start the Web server.

For more information, see your Web server documentation

2. On each Application Tier Components computer that points to the gateway on the Web server, in IBM Cognos Configuration, change the gateway URI from HTTP to HTTPS, and save the configuration.

Important: Do not start the IBM Cognos 8 service yet.

3. On each Planning Server computer that points to the gateway, in IBM Cognos Configuration, change the gateway URI from HTTP to HTTPS, and save the configuration.

Important: Do not start the IBM Cognos 8 service yet.

4. On each Application Tier Components computer, go to the *c8_location/bin* directory and import all the certificates that make up the chain of trust, in order starting with the root CA certificate, into the IBM Cognos trust store.

Import the certificates by typing the following command:

```
ThirdPartyCertificateTool.bat -T -i -r certificate_fileName -D ../configuration/signkeypair -p password
```

Note: The password should have already been set. If not, the default password is NoPassWord-Set.

5. On each Planning Server computer, go to the *c8_location/bin* directory and import all the certificates that make up the chain of trust, in order starting with the root CA certificate, into the IBM Cognos trust store.

Import the certificates by typing the following command:

```
ThirdPartyCertificateTool.bat -T -i -r certificate_fileName -D ../configuration/signkeypair -p password
```

Note: The password should have already been set. If not, the default password is NoPassWord-Set.

6. On each Application Tier Components computer, in IBM Cognos Configuration, start the IBM Cognos 8 service.
7. On each Planning Server computer, in IBM Cognos Configuration, start the IBM Cognos 8 service.

To avoid being prompted by a security alert for each new session, install the certificate into one of your Web browser's certificate stores.

In addition, you may want to set up SSL connections between IBM Cognos components and other servers. You must ensure that SSL is set up for the other servers and then you must set up a shared trust between IBM Cognos components and the other servers.

Changing the Gateway

To improve Web server performance, you can configure IBM Cognos 8 to use alternate gateways that replace the default CGI program. You can use one of the following gateways:

- Microsoft Internet Application Programming Interface (ISAPI) for Microsoft Internet Information Services on Windows
- [Apache Web Server](#) module

There is no additional Web server configuration required to use ISAPI. To access IBM Cognos 8 components using ISAPI, in IBM Cognos Configuration, change the **cognos.cgi** portion of the Gateway URI property to **cognosisapi.dll**. Then specify the ISAPI URI, **http://host_name/cognos8/isapi**, in your browser.

Before you change the gateway, we recommend that you first ensure that the default CGI gateway and your configuration work in your environment.

Configure the Gateway for IBM Cognos Apache Web Server Module

IBM Cognos 8 provides three Apache modules. The IBM Cognos Apache module requires Apache Server 1.3.x and the IBM Cognos Apache 2 module requires Apache Server 2.0.x. The IBM Cognos Apache 2.2 module requires Apache Server 2.2.x.

Steps

1. Stop Apache Web Server.
2. Append the *c8_location/cgi-bin* directory to the appropriate environment variable:
 - On Solaris or Linux, LD_LIBRARY_PATH
 - On HP-UX,
 - For Apache 1.3, SHLIB_PATH
 - For Apache 2.0 and Apache 2.2.x, SHLIB_PATH and LD_LIBRARY_PATH
 - On AIX, LIBPATH
3. On HP-UX PA-RISC, do the following:

- Ensure that the LD_PRELOAD environment variable contains /usr/lib/libcl.2.
- For Apache 1.3, set the COG_CGIBIN_DIR environment variable to *c8_location/cgi-bin*.

4. Go to the *Apache_installation/conf* directory.
5. Open the httpd.conf file in an editor.
6. Add the following to the end of the load module list:

LoadModule cognos_module "c8_location/cgi-bin/module_name"

where *module_name* is as follows:

Operating system	Apache 1.3 module	Apache 2.0 module	Apache 2.2 module
Windows	mod_cognos.dll	mod2_cognos.dll	mod2_2_cognos.dll

7. For Apache 1.3, add the following to the end of the add module list:

AddModule mod_cognos.cpp

8. Add the following to the aliases section:

```
ScriptAlias /cognos8/cgi-bin "c8_location/cgi-bin"
```

```
Alias /cognos8 "c8_location/webcontent"
```

```
<Directory "c8_location/webcontent">
```

```
Options Indexes MultiViews
```

```
</Directory>
```

The <Directory> directive is optional.

Tip: Ensure that you define the cognos8/cgi-bin alias before the cognos8 alias.

9. For Apache 2.2, add the following security rules:

```
ScriptAlias /cognos8/cgi-bin "c8_location/cgi-bin"
```

```
Alias /cognos8 "c8_location/webcontent"
```

```
<Directory "c8location/webcontent">
```

```
Options Indexes MultiViews
```

```
AllowOverride None
```

```
Options None
```

```
Order allow,deny
```

```
Allow from all
```

```
</Directory>
```

```
<Directory "c8location/cgi-bin">
```

```
AllowOverride None
```



```
Options None
Order allow,deny
Allow from all
</Directory>
```

10. For Apache 1.3 and Apache 2.0, add the following to the server status reports section:

```
<Location /cognos8/cgi-bin/cognos_module>
    SetHandler cognos-handler
</Location>
```

For Apache 2.2.x, add the following to the server status reports section:

```
<Location /cognos8/cgi-bin/cognos_module>
    SetHandler cognos-handler
Order allow,deny
Allow from all
</Location>
```

Enter the code exactly as specified. The "cognos_module" string refers to the module that you loaded in step 6.

11. For Apache 1.3 and Apache 2.0, to enable the gateway diagnostic page, add the following to the server status reports section:

```
<Location /cognos8/cgi-bin/diag_cognos_module>
    SetHandler cognos-handler
</Location>
```

For Apache 2.2.x, add the following to the server status reports section:

```
<Location /cognos8/cgi-bin/cognos_module>
    SetHandler cognos-handler
Order allow,deny
Allow from all
</Location>
```

Enter the code exactly as specified. The `diag_` string is required and the "cognos_module" string refers to the module that you loaded in step 6.

12. For Apache 1.3, add the following to the user directory section:

```
<IfModule mod_cognos.cpp>
    CgiBinDir "c8_location/cgi-bin"
</IfModule>
```

13. For Apache 2.0, add the following to the user directory section:

```
<IfModule mod_cognos.c>
    CgiBinDir "c8_location/cgi-bin"
</IfModule>
```

For Apache 2.2.x, add the following to the user directory section:

```
<IfModule mod2_2_cognos.c.c>
```

```
CGIBinDir "c8_location/cgi-bin"  
</IfModule>
```

14. Save and close the file.
15. For Apache 2.0, on HP-UX, enable searching for LD_LIBRARY_PATH by running the following command in the *Apache_installation/bin* directory:
chatr +s enable +b enable httpd
16. Start Apache Web Server.
17. In IBM Cognos Configuration, configure the **Gateway URI** property to use the *apache_mod* gateway:
http://host_name:port/cognos8/cgi-bin/module_name
where *module_name* matches the name that you used in step 6.

Configure an IBM Cognos 8 UNIX Gateway for IBM Cognos 8 Planning

If you have an IBM Cognos 8 environment running on UNIX, you can configure your UNIX gateway for IBM Cognos 8 Planning rather than using two separate gateways.

To configure the gateway for IBM Cognos 8 Planning, you must copy files from the installation files to the *c8_location* on your IBM Cognos 8 gateway computer.

Steps

1. Copy the planning gateway files to the UNIX gateway computer.
 - In the installation source directory or on the IBM Cognos 8 Planning Server CD, go to the *zipfiles\win32* directory.
 - Extract the zip file whose name begins with *planwd-win32-gate-* to a temporary directory.
 - FTP the extracted *webcontent\contributor* folder to the *c8_location/webcontent* directory on your UNIX gateway computer.
 - FTP the contents of the extracted *vers* folder to the *c8_location/vers* directory on your UNIX gateway computer.
2. Copy the planning gateway files to the UNIX gateway computer.
 - In the installation source directory or on the IBM Cognos 8 Planning Server CD, go to the *zipfiles\win32* directory.
 - Extract the zip file whose name begins with *hal-win32-gate-* to a temporary directory.
 - FTP the extracted *webcontent\hal* folder to the *c8_location/webcontent* directory on your UNIX gateway computer.
 - FTP the contents of the extracted *webcontent\skins* folder to the *c8_location/webcontent* directory on your UNIX gateway computer.
3. Copy the Contributor documentation to the UNIX gateway computer.

- In the installation source directory or on the IBM Cognos 8 Planning Server CD, go to the `zipfiles\win32` directory.
 - Extract the zip files whose names begin with `doccontribweb`, `docplanclientinst`, and `docplanningrdm` to a temporary directory.
 - FTP the extracted `webcontent\documentation` folder to the `c8_location/webcontent` directory on your UNIX gateway computer.
 - FTP the contents of the extracted `vers` folder to the `c8_location/vers` directory on your UNIX gateway computer.
4. On your UNIX gateway computer, add the component version information for the files that you copied.
 - Go to the `c8_location/vers` directory and note the version number at the end of one of the `planwd-win32-gate-` file names; for example, `8.3.###`.
 - Go to the `c8_location` directory, and open the file named `cmplst.txt` in a text editor.
 - On a new line, type the following text, including the version number you noted:
`EPCONTRIBUTORSERVER_WEBDOWNLOADGATE_version= EPCONTRIBUTORSERVERWEBDOWNLOADGATE-AW-ML-RTM-8.3.###.##`
 - On a new line, type the following text:
`EPCONTRIBUTORSERVER_WEBDOWNLOADGATE_name= Contributor Server Gateway Web Download`
 5. Configure your Planning Server and client computers to point to the UNIX gateway URI.

Configuring IBM Cognos 8 Planning to Work with Other IBM Cognos Products

Some IBM Cognos products provide functionality that is not available in IBM Cognos 8 Planning. You can continue to use these products in the same environment. Additional configuration tasks may be required to ensure that IBM Cognos 8 Planning can access objects that were created using other IBM Cognos products. Additional requirements for access depend on how you choose to run the two products.

Accessing Product Documentation in an Integrated Environment

The documentation for IBM Cognos 8 components is installed with the gateway component. If you integrate different IBM Cognos 8 products, you can either use the same gateway or use separate gateways. If you want to use the same gateway, all gateway components must be of the same product version, and you should install the IBM Cognos 8 gateway component for each product into the same location on the same computer. This ensures that all the product documentation is available to all users. If you want to use separate gateways for each product, you can install the IBM Cognos 8 gateway component for each product on separate computers, but the product documentation on each gateway will be specific for the IBM Cognos 8 product that you installed.

For example, you installed IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning using separate gateways but sharing the same content store. When users access IBM Cognos Connection, both Report Studio and Contributor are available, assuming that they have permission for both components. If users access Report Studio through the IBM Cognos 8 Business Intelligence gateway, they can use the component and access the documentation for that component. However, if users access Report Studio through the IBM Cognos 8 Planning gateway, they can use the component but do not have access to the Report Studio documentation.

If you want users to access each IBM Cognos 8 product through separate gateways, yet still be able to access documentation for all components, install the gateway component for each product into the same location as your other IBM Cognos 8 gateway components.

Configuring IBM Cognos 8 Components to Use a Another Certificate Authority

By default, IBM Cognos 8 components use their own certificate authority (CA) service to establish the root of trust in the IBM Cognos security infrastructure. You can configure IBM Cognos 8 components to use another certificate authority, if you already have an existing certificate authority, such as iPlanet or Microsoft, in your reporting environment.

When you configure IBM Cognos 8 components to use another certificate authority, ensure that you specify the same information in both the command line utility tool and in IBM Cognos Configuration.

To configure IBM Cognos 8 components to use another certificate authority, you must

- ☐ [generate IBM Cognos security keys and certificate signing requests](#) to use with your CA
- ☐ submit the IBM Cognos security keys and certificates to your certificate authority
- ☐ [configure IBM Cognos 8 components to use a your certificate authority](#)

Generate Keys and Certificate Signing Requests

Use the command line utility to generate all the keys for the IBM Cognos key stores and to generate the certificate signing requests (CSR).

The following table lists the options for the command-line tool used to generate keys and signing requests.

Command	Description
Main operation mode	
-c	Create a new CSR
-i	Import a certificate
Operation modifiers	

Command	Description
-s	Work with the signing identity
-e	Work with the encryption identity
-T	Work with the trust store (only with -i)
Information Flags	
-d	DN to use for certificate
-r	CSR or certificate file location (depends on mode)
-t	certificate authority certificate file (only with -i)
-p	Key Store password (must be provided)
-a	Key pair algorithm. RSA or DSA. Default: RSA
-D	Directory location

The following sample values are used:

Property	Value
Signing certificate DN	CN=SignCert,O=MyCompany,C=CA
Encryption certificate DN	CN=EncryptCert,O=MyCompany,C=CA
Key store password	password

Steps

1. In the *c8_location*\configuration directory, back up the cogstartup.xml file to a secure location.
2. Back up the contents of the following directories to a secure location:
 - *c8_location*\configuration\signkeypair
 - *c8_location*\configuration\encryptkeypair
3. Using IBM Cognos Configuration, export the configuration in clear text by doing the following:
 - Open IBM Cognos Configuration.
 - From the **File** menu, click **Export As**.

- When prompted about exporting decrypted content, click **Yes**.
 - In the **Export As** dialog box, select `cogstartup.xml` and then click **Save**.
 - When prompted about replacing the existing file, click **Yes**.
 - When the tasks are complete, close the IBM Cognos Configuration dialog box.
 - Save the configuration.
 - Close IBM Cognos Configuration.
4. Go to the `c8_location\bin` directory.
 5. Create the certificate signing request for the signing keys by typing the following command:
On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -c -s -d "CN=SignCert,O=MyCompany,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p password
```


On Windows, type

```
ThirdPartyCertificateTool.bat c -s -d "CN=SignCert,O=MyCompany,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p password
```

Tip: UNIX or Linux filenames are case-sensitive and must be entered exactly as shown.

You can safely ignore any warnings about logging.

The command creates the `jSignKeystore` file in the `signkeypair` directory, sets the specified password, creates a new keypair and stores it in the keystore, and exports the `signRequest.csr` file to the `c8_location\bin` directory.
 6. Create the certificate signing request for the encryption keys by typing the following command:
On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r encryptRequest.csr -D ../configuration/encryptkeypair -p password
```


On Windows, type

```
ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r encryptRequest.csr -D ../configuration/encryptkeypair -p password
```

You can safely ignore any warnings about logging.

The command creates the `jEncKeystore` file in the `encryptkeypair` directory, sets the specified password, creates a new keypair and stores it in the keystore, and exports the `encryptRequest.csr` file to the `c8_location\bin` directory.
 7. Copy the `signRequest.csr` and `encryptRequest.csr` files that were generated in steps 5 and 6 to a directory that is accessible by your certificate authority.
 8. Input the `signRequest.csr` and `encryptRequest.csr` files into the certificate authority.
The certificate authority produces a signing certificate and an encryption certificate.
For more information, see your CA documentation.

9. Copy the contents of the signing certificate into a file named `signCertificate.cer`.
10. Copy the contents of the encryption certificate into a file named `encryptCertificate.cer`
11. Find the root CA certificate for the certificate authority and copy the contents into a file named `ca.cer`.
12. Copy `ca.cer`, `signCertificate.cer`, and `encryptCertificate.cer` to `c8_location/bin`.

These files must be PEM (Base-64 encoded ASCII) format.

13. Import the signing certificate from step 10 into the IBM Cognos signing key store by typing the following command:

On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -i -s -r signCertificate.cer -D ../configuration/signkeypair -p  
password -t ca.cer
```

On Windows, type

```
ThirdPartyCertificateTool.bat -i -s -r signCertificate.cer -D ../configuration/signkeypair -p  
password -t ca.cer
```

You can safely ignore any warnings about logging.

The command reads the `signCertificate.cer` and `ca.cer` files in the `c8_location\bin` directory and imports the certificates from both files into the `jSignKeystore` file in the `signkeypair` directory using the specified password.

14. Import the encryption certificate from step 11 into the IBM Cognos encryption key store by typing the following command:

On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair  
-p password -t ca.cer
```

On Windows, type

```
ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair  
-p password -t cacert.cer
```

You can safely ignore any warnings about logging.

The command reads the `encryptCertificate.cer` and `ca.cer` files in the `c8_location\bin` directory and imports the certificates from both files into the `jEncKeystore` file in the `encryptkeypair` directory using the specified password.

15. Import the CA certificate from step 12 into the IBM Cognos trust store by typing the following command:

On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -i -T -r ca.cer -D ../configuration/signkeypair -p password
```

On Windows, type

```
ThirdPartyCertificateTool.bat -i -T -r ca.cer -D ../configuration/signkeypair -p password
```

The command reads the ca.cer file and imports the contents into the jCAKeystore file in the signkeypair directory using the specified password.

The certificates are now ready to be [configured for IBM Cognos 8](#).

Configure IBM Cognos 8 Components to Run Within Another Certificate Authority

You must configure each IBM Cognos computer to use an external certificate authority by setting the appropriate property in IBM Cognos Configuration.

By setting this property, IBM Cognos 8 components assume that all required keys have been generated and vetted by the external certificate authority.

Ensure that the key store locations and password in IBM Cognos Configuration match the ones you typed in the command-line tool.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Cryptography**, click **IBM Cognos**.
3. In the **Properties** window, under **Certificate Authority settings** property group, click the **Value** box next to the **Use third party CA** property and then click **True**.

Note: When you set this property to true, all properties for the certificate authority and identity name are ignored.

4. Configure the following properties to match the ones you typed in the command line utility:
 - **Signing key store location**
 - **Signing key store password**
 - **Encryption key store location**
 - **Encryption key store password**
 - **Certificate Authority key store password**
5. From the **File** menu, click **Save**.
6. If you want to start the IBM Cognos 8 service, from the **Actions** menu, click **Start**.

This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Tuning Techniques for Improving Performance

Changes in your environment can affect the performance of IBM Cognos Planning. Therefore, it is important to monitor and tune performance regularly. Monitoring performance means regularly gathering data about your usage and response times.

For more information about performance tuning, see the IBM Cognos 8 Planning *Architecture and Planning Guide*.

Tuning a DB2 Content Store

If you use a DB2 database for the content store ([p. 44](#)), you can take steps to improve the speed with which requests are processed.

By default, DB2 assigns tables that contain large objects (LOBS) to a database-managed tablespace. As a result, the LOBS are not managed by the DB2 buffer pools. This results in direct I/O requests on the LOBS, which affects performance. By reassigning the tables that contain LOBS to a system-managed tablespace, you reduce the number of direct I/O requests.

Before changing a DB2 content store, allocate sufficient log space to restructure the database. To reconfigure the DB2 content store, do the following:

- ☐ Export the data from the tables that contain at least one large object (LOB).
- ☐ Create the tables in a system-managed table space.
- ☐ Import the data into the tables.

Chapter 10: Configuring IBM Cognos 8 Components to Use an Authentication Provider

IBM Cognos 8 components run with two levels of logon: anonymous and authenticated. By default, anonymous access is enabled.

You can use both types of logon with your installation. If you choose to use only authenticated logon, you can disable anonymous access.

For authenticated logon, you must configure IBM Cognos 8 components with an appropriate namespace for the type of authentication provider in your environment. You can configure multiple namespaces for authentication and then choose at run time which namespace you want to use. For more information, see the *Administration and Security Guide*.

IBM Cognos 8 components support the following types of servers as authentication sources:

- [Active Directory Server](#)
- [IBM Cognos Series 7](#)
- [Custom Authentication Provider](#)
- [LDAP](#)
- [eTrust SiteMinder](#)
- [NTLM](#)
- [SAP](#)

If you use more than one Content Manager computer, you must configure identical authentication providers on each Content Manager computer. This means that the type of authentication provider you select and the way you configure it must be identical on all computers for all platforms. The configuration must contain information that is accessible by all Content Manager computers.

If you enable security, you must configure security settings immediately after you complete the installation and configuration process. For more information, see the *Administration and Security Guide*.

Important: We recommend that you do not disable security after you enable it. If you delete a namespace, the user preferences, My Folders, and My Pages entries are permanently lost. Existing permission settings will refer to users, groups or roles that no longer exist. While this does not affect how the permissions work, a user administering the permission settings may see "unknown" entries. Because these entries refer to users, groups, and roles which no longer exist, you can safely delete them.

After you configure an authentication provider for IBM Cognos 8 components, you can enable single signon between your authentication provider environment and IBM Cognos 8 components. This means that a user logs on once and can then switch to another application without being asked to log on again.

Users can select namespaces when they log in to the IBM Cognos 8 portal. You can hide Custom Java namespaces (p. 159) and eTrust SiteMinder namespaces (p. 177) from users.

To use an authentication provider and to require users to authenticate:

- ❑ [Disable anonymous access](#), if required.
- ❑ Configure IBM Cognos 8 components to use an authentication provider.

Disable Anonymous Access

By default, users are not required to log in to IBM Cognos 8. To use IBM Cognos 8 Planning, you must disable anonymous access so that users are required to log in only authenticated users can access your planning applications.

Steps

1. On each Content Manager computer, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, click **IBM Cognos**.

The IBM Cognos resource represents the IBM Cognos namespace. The IBM Cognos namespace stores information about IBM Cognos groups, such as the Anonymous User, contacts, and distribution lists, and refers to objects in other security namespaces. For more information, see the *Administration and Security Guide*.
3. In the **Properties** window, click the box next to the **Allow anonymous access** property and then click **False**.
4. From the **File** menu, click **Save**.

Now, users are required to provide logon credentials when they access IBM Cognos resources.

Restrict User Access to the IBM Cognos Namespace

Access can be restricted to users belonging to any group or role defined in the IBM Cognos built-in namespace. By default, all users belong to several built-in groups or roles. To restrict access, you must:

- enable the property to restrict access
- remove the Everyone group from the IBM Cognos built-in roles and groups
- ensure that authorized users belong to at least one IBM Cognos role or group

Steps

1. On each Content Manager computer, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Authentication**.
3. In the **Properties** window, change the value of **Restrict access to members of the built-in namespace** to **True**.

4. From the **File** menu, click **Save**.

You must now use the portal to remove the Everyone group from the IBM Cognos built-in roles and groups and then ensure that authorized users belong to at least one IBM Cognos built-in role or group.

For information about adding or removing members of an IBM Cognos group or role, see the *Administration and Security Guide*.

Configuring IBM Cognos 8 Components to Use Active Directory Server

If you install Content Manager on a Windows computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

For more information, see ["Configure an LDAP Namespace for Active Directory Server" \(p. 162\)](#).

If you want to use Microsoft SQL Server or Microsoft Analysis Server as a data source and use single signon for authentication, you must use Active Directory as your authentication source.

You cannot connect to the Active Directory Global Catalog, which is a caching server for Active Directory Server. If the connection uses port 3268, you must change it. By default, Active Directory Server uses port 389.

To use an Active Directory Server namespace and to set up single signon, do the following:

- ☐ [Configure IBM Cognos 8 components to use an Active Directory Server namespace](#)
- ☐ [Enable secure communication to the Active Directory Server](#), if required
- ☐ [Enable single signon between Active Directory Server and IBM Cognos 8 components](#)

Configure an Active Directory Namespace

You can use Active Directory Server as your authentication provider.

You also have the option of making custom user properties from the Active Directory Server available to IBM Cognos 8 components.

For IBM Cognos 8 to work properly with Active Directory Server, you must ensure that the Authenticated users group has Read privileges for the Active Directory folder where users are stored.

If you are configuring an Active Directory namespace to support single signon with a Microsoft SQL Server or Microsoft Analysis Server data source, the following configuration is required:

- The IBM Cognos 8 gateway must be installed on an IIS Web server that is configured for Windows Integrated Authentication.
- The gateway must be assigned to the local intranet Web site in your Web browser.
- Content Manager must be installed on a Windows 2000 or Windows 2003 server.
- Content Manager, the report server (Application Tier Components), IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server) must belong to the Active Directory domain.

- The data source connection for Microsoft SQL Server or Microsoft Analysis Server must be configured for **External Namespace** and that namespace must be the Active Directory namespace.

For more information about data sources, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.
7. Specify the values for the **Host and port** property.

To support Active Directory Server failover, you can specify the domain name instead of a specific domain controller. For example, use *mydomain.com:389* instead of *dc1.mydomain.com:389*.

8. If you want to be able to search for details when authentication fails, specify the user ID and password for the **Binding credentials** property.

Use the credentials of an Active Directory Server user who has search and read privileges for that server.

9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Make Custom User Properties for Active Directory Available to IBM Cognos 8 Components

You can use arbitrary user attributes from your Active Directory Server in IBM Cognos 8 components. To configure this, you must add these attributes as custom properties for the Active Directory namespace.

The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the Framework Manager *User Guide*

The custom properties can also be used inside command blocks that are used to configure Oracle sessions and connections. The command blocks can be used with Oracle light-weight connections and virtual private databases. For more information, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, click the Active Directory namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties** and click the edit button.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column and enter the name you want IBM Cognos 8 components to use for the session parameter.
6. Click the **Value** column and enter the name of the account parameter in your Active Directory Server.
7. Repeat steps 4 to 6 for each custom parameter.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Enabling Secure Communication to the Active Directory Server

If you are using an SSL connection to the Active Directory Server, you must copy the certificate from the Active Directory Server to the Content Manager computer.

Steps

1. On every Content Manager computer, use your Web browser to connect to the Active Directory Server and copy the CA root certificate to a location on the Content Manager computer.
2. Add the CA root certificate to the certificate store of the account that you are using for the current IBM Cognos session:
 - If you are running the IBM Cognos session under a user account, use the same Web browser as in step 1 to import the CA root certificate to the certificate store for your user account. For information, see the documentation for your Web browser.
 - If you are running the IBM Cognos session under the local computer account, use Microsoft Management Console (MMC) to import the CA root certificate to the certificate store for the local computer. For information, see the documentation for MMC.
3. In IBM Cognos Configuration, restart the service:
 - In the **Explorer** window, click **IBM Cognos 8 service, IBM Cognos 8**.
 - From the **Actions** menu, click **Restart**.

Include or Exclude Domains Using Advanced Properties

When you configure an authentication namespace for IBM Cognos 8, users from only one domain can log in. By using the Advanced properties for Active Directory Server, users from related (parent-child) domains and unrelated domain trees within the same forest can also log in.

Authentication in One Domain Tree

If you set a parameter named `chaseReferrals` to true, users in the original authenticated domain and all child domains of the domain tree can log in to IBM Cognos 8. Users above the original authenticated domain or in a different domain tree cannot log in.

Authentication in All Domain Trees in the Forest

If you set a parameter named `MultiDomainTrees` to true, users in all domain trees in the forest can log in to IBM Cognos 8.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, click the Active Directory namespace.
3. In the **Properties** window, specify the **Host and port** property:
 - For users in one domain, specify the host and port of a domain controller for the single domain.
 - For users in one domain tree, specify the host and port of the top-level controller for the domain tree.
 - For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.
4. Click in the Value column for **Advanced properties** and click the edit button.
5. In the **Value - Advanced properties** window, click **Add**.
6. Specify two new properties, `chaseReferrals` and `MultiDomainTrees`, with the following values:

Authentication for	<code>chaseReferrals</code>	<code>MultiDomainTrees</code>
One domain	False	False
One domain tree	True	False
All domain trees in the forest	True	True

7. Click **OK**.
8. From the **File** menu, click **Save**.

Enabling Single Signon Between Active Directory Server and IBM Cognos 8 Components

By default, the Active Directory provider uses Kerberos delegation and integrates with the IIS Web server for single signon if Windows integrated authentication (formerly named NT Challenge Response) is enabled on the IIS Web server.

If Windows integrated authentication is enabled, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the Active Directory namespace.

If you do not want Kerberos delegation, the provider can be configured to access the environment variable REMOTE_USER to achieve single signon. You must set the advanced property singleSignOnOption to the value IdentityMapping. You must also specify bind credentials for the Active Directory namespace. Microsoft sets REMOTE_USER by default when you enable Windows integrated authentication. If Kerberos authentication is bypassed, single signon to Microsoft OLAP (MSAS) data sources will not be possible.

Steps for Single Signon Using Kerberos Delegation

1. Set up Windows integrated authentication on the IIS Web server.
2. Install Content Manager on a computer that is part of the domain, for the active and standby Content Manager computers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted for delegation.

When setting up the computers using the Active Directory user tool, do not select the **Account** attribute, which is sensitive and cannot be delegated.

Steps for Single Signon Using REMOTE_USER

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, click the Active Directory namespace.
3. Click in the **Value** column for **Advanced properties** and then click the edit button.
4. In the **Value - Advanced properties** dialog box, click **Add**.
5. In the **Name** column, type **singleSignOnOption**
6. In the **Value** column, type **IdentityMapping**.
7. Click **OK**.
8. Click in the **Value** column for **Binding credentials**, and then click the edit button.
9. In the **Value - Binding credentials** dialog box, specify a user ID and password and then click **OK**.

The Active Directory provider now uses REMOTE_USER for single signon.

Tip: To switch back to Kerberos delegation, edit **Advanced properties** and, in the **Value** column, type **KerberosAuthentication**.

Configuring IBM Cognos 8 to Use IBM Cognos Series 7 Namespace

You can configure IBM Cognos 8 components to use an IBM Cognos Series 7 namespace as the authentication provider. Users will be authenticated based on the authentication and signon configuration of the IBM Cognos Series 7 namespace.

Note: You cannot use an IBM Cognos Series 7 Local Authentication Export (LAE) file for authentication with IBM Cognos 8 components.

You can configure IBM Cognos 8 components to use multiple IBM Cognos Series 7 authentication providers. We recommend that all IBM Cognos Series 7 namespaces use the same primary IBM Cognos Series 7 Ticket Server. Otherwise, you may receive errors or be prompted for authentication more than once. To maintain performance, also ensure that the ticket server is running.

If you change the configuration information stored in the directory server used for IBM Cognos Series 7, you must restart the IBM Cognos 8 service before the changes take effect in the IBM Cognos installation.

A user must be in at least one Access Manager user class to be able to log on to IBM Cognos 8 components.

To use an IBM Cognos Series 7 namespace and to set up single signon, do the following:

- ❑ [Configure IBM Cognos 8 to use an IBM Cognos Series 7 namespace](#)
- ❑ [Enable secure communication to the directory server used by the IBM Cognos Series 7 namespace](#), if required
- ❑ [Enable single signon between IBM Cognos Series 7 and IBM Cognos 8](#)

Configure an IBM Cognos Series 7 Namespace

You can configure IBM Cognos 8 to use one or more IBM Cognos Series 7 namespaces for authentication.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.
The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.

If your IBM Cognos Series 7 namespace version is 16.0, ensure that the **Data encoding** property is set to **UTF-8**. In addition, the computers where Content Manager is installed must use the same locale as the data in the IBM Cognos Series 7 namespace.

The host value can be a computer name or an IP address. If you are publishing from PowerPlay Enterprise Server to IBM Cognos 8, you must use the same value format that is used in IBM Cognos Series 7 Configuration Manager for the location of the directory server. For example, if the computer name is used in IBM Cognos Series 7 Configuration Manager, the computer name must also be used in IBM Cognos Configuration for IBM Cognos 8.

7. If your namespace environment includes version 15.2 of the IBM Cognos Series 7 namespace, you must disable the **Series7NamespacesAreUnicode** setting.
 - In the **Properties** window, in the **Advanced Properties** value, click the edit button.
 - In the **Value - Advanced properties** window, click **Add**.
 - In the **Name** box, type **Series7NamespacesAreUnicode**.
 - In the **Value** box, type **False**, and then click **OK**.
8. In the **Properties** window, under **Cookie settings**, ensure that the **Path**, **Domain**, and **Secure flag enabled** properties match the settings configured for IBM Cognos Series 7.
9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace

If you are using an SSL connection to the Directory Server used by the IBM Cognos Series 7 namespace, you must copy the certificate from the Directory Server to each Content Manager computer.

For more information, see the IBM Cognos Access Manager *Administrator Guide* and the documentation for your Directory Server.

Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos 8

If your IBM Cognos Series 7 namespace has been configured for integration with your external authentication mechanisms for single signon, the IBM Cognos Series 7 provider will automatically use this configuration.

By configuring single signon, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the IBM Cognos Series 7 namespace.

Steps

1. Ensure that you configured IBM Cognos 8 components to use an IBM Cognos Series 7 namespace as an authentication provider ([p. 154](#)).
2. For IBM Cognos Series 7, start Configuration Manager.
3. Click **Open the current configuration**.
4. On the **Components** tab, in the **Explorer** window, expand **Services, Access Manager - Runtime** and click **Cookie Settings**.
5. In the **Properties** window, ensure that the **Path**, **Domain**, and **Secure Flag Enabled** properties match the settings configured for IBM Cognos 8.
6. Save and close Configuration Manager.
7. If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must now [define the SaferAPIGetTrustedSignonWithEnv function](#).

You can now add IBM Cognos Upfront Series 7 NewsBoxes to your IBM Cognos Connection portal pages.

IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in

If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must define the `SaferAPIGetTrustedSignonWithEnv` function in your plug-in. Then you must recompile and redeploy the library for single signon to be achieved between IBM Cognos 8 components and your authentication mechanism.

The `SaferAPIGetTrustedSignonWithEnv` function is an updated version of the `SaferAPIGetTrustedSignon` function. This update is required because IBM Cognos 8 login is not performed at the Web server as is the case for IBM Cognos Series 7 applications. Therefore, it is not possible for the plug-in to perform a `getenv()` API call to retrieve Web server environment variables. The plug-in can request that specific environment variables be removed from the Web server using the `SaferAPIGetTrustedSignonWithEnv` function.

If you are running both IBM Cognos Series 7 and IBM Cognos 8 products using the same plug-in, both the `SaferAPIGetTrustedSignonWithEnv` and `SaferAPIGetTrustedSignon` functions are required. For information about the `SaferAPIGetTrustedSignon` function, see the IBM Cognos Series 7 documentation.

SaferAPIGetTrustedSignonWithEnv Function

For users to be successfully authenticated by Access Manager, OS signons must exist and be enabled in the current namespace.

The memory for the returned `trustedSignonName` and `trustedDomainName` is allocated internally in this API. If the function returns `SAFER_SUCCESS`, Access Manager calls `SaferAPIFreeTrustedSignon` to free the memory allocated.

The memory for the returned `reqEnvVarList` is allocated internally in this API. If the function returns `SAFER_INFO_REQUIRED`, Access Manager calls `SaferAPIFreeBuffer()` to free the memory allocated.

Both functions, `SaferAPIGetTrustedSignon` and `SaferAPIFreeBuffer` must be implemented to successfully register the library when `SaferAPIGetTrustedSignonWithEnv` is implemented. The function `SaferAPIGetError` is required only if you want specific error messages returned from your plug-in.

Syntax

`SaferAPIGetTrustedSignonWithEnv(`

<code>EnvVar</code>	<code>envVar[],</code>	<code>/*[IN]*/</code>
<code>char</code>	<code>**reqEnvVarList,</code>	<code>/*[OUT]*/</code>
<code>void</code>	<code>**trustedSignonName,</code>	<code>/*[OUT]*/</code>
<code>unsigned long</code>	<code>*trustedSignonNameLength,</code>	<code>/*[OUT]*/</code>
<code>void</code>	<code>**trustedDomainName,</code>	<code>/*[OUT]*/</code>
<code>unsigned long</code>	<code>*trustedDomainNameLength,</code>	<code>/*[OUT]*/</code>
<code>SAFER_USER_TYPE</code>	<code>*userType,</code>	<code>/*[OUT]*/</code>
<code>void</code>	<code>**implementerData);</code>	<code>/*[IN/OUT]*/</code>

Parameter	Description
[in] <code>envVar</code>	An array of environment variable names and values that were retrieved from the Web server. The end of the array is represented by an entry with a null <code>envVarName</code> and a null <code>envVarValue</code> . Note that the first time this API is called, the <code>envVar</code> array contains only the end of array marker.
[in] <code>reqEnvVarList</code>	A string that contains a comma separated list of environment variable names that are requested by the Safer implementation. The end of the list must be null-terminated.
[out] <code>trustedSignonName</code>	A sequence of bytes that identifies the currently authenticated user. This value does not need to be null-terminated. This value is mandatory.

Parameter	Description
[out] trustedSignonNameLength	An integer value that indicates the length of the trusted-SignonName. This length should exclude the null terminator, if there is one. This value is mandatory.
[out] trustedDomainName	A sequence of bytes that identifies the domain of the currently authenticated user. This value does not need to be null-terminated. If there is no trustedDomainName, the return is null. This value is optional.
[out] trustedDomainNameLength	An integer value that indicates the length of the trustedDomainName. This length should exclude the null terminator, if there is one. This value is mandatory and must be set to zero if there is no trustedDomainName.
[out] userType	<p>A value that indicates the type of user that Access Manager will authenticate. This value is mandatory.</p> <p>The following return values are required for users to be successfully authenticated by Access Manager:</p> <p>SAFER_NORMAL_USER</p> <p>A named user. OS signons must exist and be enabled in the current namespace.</p> <p>SAFER_GUEST_USER</p> <p>A guest user. A guest user account must exist and be enabled in the current namespace.</p> <p>SAFER_ANONYMOUS_USER</p> <p>An anonymous user. An anonymous user account must exist and be enabled in the current namespace.</p>
[in/out] implementerData	A pointer used to preserve implementation-specific data between invocations. An invocation occurs every time Access Manager calls the trusted signon plug-in. This value is valid only if the trusted signon plug-in was invoked and you set a value for it.

Configuring IBM Cognos 8 to Use a Custom Authentication Provider

If you implemented a custom Java authentication provider with your existing security infrastructure, you can configure IBM Cognos 8 components to use it.

You can use a custom authentication provider to access and authenticate users to an alternate authentication source. You can also use it as a single signon mechanism to integrate IBM Cognos 8 components with your security infrastructure. You can hide the namespace from users during logon.

For more information, see the Custom Authentication Provider *Developer Guide*.

Configure a Custom Authentication Namespace

You can configure IBM Cognos 8 components to use a custom authentication namespace. Any additional configuration for authentication source access, single signon, or custom attributes are dependent on the custom authentication provider implementation.

Steps

1. On every computer where installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **Custom Java Provider** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 can locate and use your existing authentication provider.
7. From the **File** menu, click **Save**.
8. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Hide the Namespace from Users During Login

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users log in.

For example, you may want to integrate single signon across systems but maintain the ability for customers to authenticate directly to IBM Cognos 8 without being prompted to choose a namespace.

Steps

1. On each computer where you configured a custom Java authentication provider, open IBM Cognos Configuration.

2. In the **Explorer** window, under **Security, Authentication**, click the custom Java authentication provider.
3. In the **Properties** window, click the box next to **Selectable for authentication?** and then click **False**.
4. From the **File** menu, click **Save**.

The namespace is not shown on the selection list that is presented at login.

Configuring IBM Cognos 8 Components to Use LDAP

You can configure IBM Cognos 8 components to use an LDAP namespace as the authentication provider. You can use an LDAP namespace for users that are stored in an LDAP user directory, Active Directory Server, IBM Directory Server, Novell Directory Server, or Sun Java System Directory Server.

You can also use LDAP authentication with DB2 and Essbase OLAP data sources by specifying the LDAP namespace when you set up the data source connection. For more information, see the *Administration and Security Guide*.

You also have the option of making custom user properties from the LDAP namespace available to IBM Cognos 8 components.

To bind a user to the LDAP server, the LDAP authentication provider must construct the distinguished name (DN). If the **Use external identity** property is set to **True**, it uses the **External identity mapping** property to try to resolve the user's DN. If it cannot find the environment variable or the DN in the LDAP server, it attempts to use the **User lookup** property to construct the DN.

If users are stored hierarchically within the directory server, you can configure the **User lookup** and **External identity mapping** properties to use search filters. When the LDAP authentication provider performs these searches, it uses the filters you specify for the **User lookup** and **External identity mapping** properties. It also binds to the directory server using the value you specify for the **Bind user DN and password** property or using **anonymous** if no value is specified.

When an LDAP namespace has been configured to use the **External identity mapping** property for authentication, the LDAP provider binds to the directory server using the **Bind user DN and password** or using **anonymous** if no value is specified. All users who log on to IBM Cognos 8 using external identity mapping see the same users, groups, and folders as the **Bind user**.

If you do not use external identity mapping, you can specify whether to use bind credentials to search the LDAP directory server by configuring the **Use bind credentials for search** property. When the property is enabled, searches are performed using the bind user credentials or using **anonymous** if no value is specified. When the property is disabled, which is the default setting, searches are performed using the credentials of the logged-on user. The benefit of using bind credentials is that instead of changing administrative rights for multiple users, you can change the administrative rights for the bind user only.

Important: If you use a DN syntax, such as `uid=${userID}, ou=mycompany.com`, for the properties **User lookup**, **External identity mapping**, or **Bind user DN and password**, you must escape all special characters that are used in the DN. If you use a search syntax, such as `(uid=${userID})`, for the

properties **User lookup** or **External identity mapping**, you must not escape special characters that are used in the DN.

To use an LDAP namespace and set up single signon, do the following:

- ❑ [Configure IBM Cognos 8 components to use an LDAP namespace](#)
- ❑ [Make custom user properties available to IBM Cognos 8 components](#), if required
- ❑ [Enable secure communication to the LDAP server](#), if required
- ❑ [Enable single signon between LDAP and IBM Cognos 8 components](#), if required

Configure an LDAP Namespace

You can configure IBM Cognos 8 components to use an LDAP namespace when the users are stored in an LDAP user directory. The LDAP user directory may be accessed from within another server environment, such as Active Directory Server or eTrust SiteMinder.

If you are configuring an LDAP namespace for a directory server other than LDAP, see the appropriate section:

- For Active Directory Server, see [Configure an LDAP Namespace for Active Directory Server](#).
- For IBM Directory Server, see [Configure an LDAP Namespace for IBM Directory Server](#).
- For Novell Directory Server, see [Configure an LDAP Namespace for Novell Directory Server](#).
- For Sun Java System Directory Server, see [Configure an LDAP Namespace for Sun Java System Directory Server](#)

You can also use LDAP authentication with DB2 and Essbase OLAP data sources by specifying the LDAP namespace when you set up the data source connection. For more information, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.

7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

If external identity mapping is enabled, **Bind user DN and password** are used for all LDAP access. If external identity mapping is not enabled, **Bind user DN and password** are used only when a search filter is specified for the **User lookup** property. In that case, when the user DN is established, subsequent requests to the LDAP server are executed under the authentication context of the end user.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
 - Ensure that **Use external identity** is set to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.

If you do not specify a user ID and password, and anonymous access is enabled, the search is done using anonymous.

9. Check the mapping settings for required objects and attributes.

Depending on the LDAP configuration, you may have to change some default values to ensure successful communication between IBM Cognos 8 components and the LDAP server.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

10. From the **File** menu, click **Save**.

11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configure an LDAP Namespace for Active Directory Server

If you configure a new LDAP namespace for use with an Active Directory Server, you must modify the necessary settings and change the values for all properties of the Active Directory objects.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.

The following settings are examples:

- For **User lookup**, specify (sAMAccountName=\${userID})
- If you use single signon, for **Use external identity**, set the value to **True**.
- If you use single signon, for **External identity mapping**, specify (sAMAccountName=\${environment("REMOTE_USER")})
If you want to remove the domain name from the REMOTE_USER variable, specify (sAMAccountName=\${replace(\${environment("REMOTE_USER")}, "domain\\", "")}).
- For **Bind user DN and password**, specify *user@domain*
- For **Unique identifier**, specify **objectGUID**

7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
 - Ensure that **Use external identity** is set to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with the Active Directory Server objects, use the values specified in the following table.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalUnit,organization,container
	Description	description
	Name	ou,o,cn

Mappings	LDAP property	LDAP value
Group	Object class	group
	Description	description
	Member	member
	Name	cn
Account	Object class	user
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	displayName
	Pager phone	pager
	Password	unicodePwd
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn
	Username	sAMAccountName

These mapping properties represent changes based on a default Active Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configure an LDAP Namespace for IBM Directory Server

If you configure a new LDAP namespace for use with an IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 can locate and use your existing authentication namespace.
 - For **User lookup**, specify `cn=${userID}`
 - For **Bind user DN and password**, specify `cn=root`
7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.
If no values are specified, the LDAP authentication namespace binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
 - Ensure that **Use external identity** is set to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.
9. To configure the LDAP advanced mapping properties for use with IBM Directory Server objects, use the values specified in the following table.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit,organization,container
	Description	description
	Name	ou,o,cn
Group	Object class	groupofnames
	Description	description
	Member	member
	Name	cn
Account	Object class	inetorgperson
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	userPassword
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn

Mappings	LDAP property	LDAP value
	Username	uid

These mapping properties represent changes based on a default IBM Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

Configure an LDAP Namespace for Novell Directory Server

If you configure a new LDAP namespace for use with a Novell Directory Server, you must modify the necessary settings and change the values for all properties of the Novell Directory objects.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 can locate and use your existing authentication namespace.
 - For **User lookup**, specify (cn=\${userID})
 - For **Bind user DN and password**, specify the base DN for an administration user, such as **cn=Admin,0=COGNOS**
7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

If no values are specified, the LDAP authentication namespace binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
 - Ensure that **Use external identity** is set to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with Novell Directory Server objects, use the values specified in the following table.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

For users to successfully log in to IBM Cognos Connection, they must have permission to read the ou and o attributes.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit,organization,container
	Description	description
	Name	ou,o,cn
Group	Object class	groupofnames
	Description	description
	Member	member
	Name	cn
Account	Object class	inetOrgPerson
	Business phone	telephonenumber
	Content locale	Language
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager

Mappings	LDAP property	LDAP value
	Password	(leave blank)
	Postal address	postaladdress
	Product locale	Language
	Surname	sn
	Username	uid

These mapping properties represent changes based on a default Novell Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

Configure an LDAP Namespace for Sun Java System Directory Server

If you configure a new LDAP namespace for use with Sun Java System Directory Server, you must modify the necessary settings and change the values for all properties of the Sun Java System Directory objects.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 can locate and use your existing authentication namespace.

The following settings are examples:

- For **User lookup**, type (uid=\${userID})
- If you use single signon, for **Use external identity**, set the value to **True**.

- If you use single signon, for **External identity mapping**, specify any attribute, such as the NT user domain ID or the user ID:

```
(ntuserdomainid=$environment("REMOTE_USER"))
```

```
(uid=${environment("REMOTE_USER")})
```

- For **Unique identifier**, type `nsuniqueid`
7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.
If no values are specified, the LDAP authentication namespace binds as anonymous.
 8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
 - Ensure that **Use external identity** is set to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.
 9. To configure the LDAP advanced mapping properties for use with Sun Java System Directory Server objects, use the values specified in the following table.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalUnit,organization
	Description	description
	Name	ou,o
Group	Object class	groupofuniquenames
	Description	description
	Member	uniquemember
	Name	cn
Account	Object class	inetorgperson
	Business phone	telephonenumber
	Content locale	preferredlanguage

Mappings	LDAP property	LDAP value
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	userPassword
	Postal address	postaladdress
	Product locale	preferredlanguage
	Surname	sn
	Username	uid

These mapping properties represent changes based on a default Sun Java System Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

Make Custom User Properties for LDAP Available to IBM Cognos 8 Components

You can use arbitrary user attributes from your LDAP authentication provider in IBM Cognos 8 components. To configure this, you must add these attributes as custom properties for the LDAP namespace. The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the Framework Manager *User Guide*.

The custom properties can also be used inside command blocks that are used to configure Oracle sessions and connections. The command blocks can be used with Oracle lightweight connections and virtual private databases. For more information, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open IBM Cognos Configuration.

2. In the **Explorer** window, under **Security, Authentication**, click the LDAP namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties** and click the edit button.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column, and enter the name you want IBM Cognos 8 components to use for the session parameter.
6. Click the **Value** column, and enter the name of the account parameter in your LDAP authentication provider.
7. Repeat the preceding two bulleted steps for each custom parameter.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Enable Secure Communication to the LDAP Server

Secure LDAP protocol (LDAPS) encrypts the communication between the Access Manager component of Content Manager and the directory server. LDAPS prevents sensitive information in the directory server and the LDAP credentials from being sent as clear text.

To enable LDAPS, install a server certificate that is signed by a certificate authority in the directory server. Next, create a certificate database to contain the certificates. Finally, configure the directory server and the IBM Cognos 8 LDAP namespace to use LDAPS.

The server certificate must be a copy of either

- the trusted root certificate and all other certificates that make up the chain of trust for the directory server certificate

The trusted root certificate is the certificate of the root certificate authority that signed the directory server certificate.

- the directory server certificate only

The certificates must be Base64 encoded in ASCII (PEM) format. All certificates except the trusted root certificate must not be self-signed.

You must use the certutil tool from Netscape OpenSource toolkit NSS_3_3_2_RTM to create the certificate database. IBM Cognos 8 does not accept other versions of cert7.db files, including those from the certutil tool that is provided with Microsoft Active Directory. The appropriate certutil tool is available from [ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM](http://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM).

For UNIX and Linux, you must also use the NSPR library, which is available from [ftp://ftp.mozilla.org/pub/mozilla.org/nspr/releases/v4.1.2](http://ftp.mozilla.org/pub/mozilla.org/nspr/releases/v4.1.2).

Steps

1. Create a directory for the certificate database.
2. Create the certificate database by typing

certutil -N -d *certificate_directory*

where *certificate_directory* is the directory that you created in step 1.

This command creates a cert7.db file and a key3.db file in the new directory.

3. Add the certificate authority (CA) certificate or the directory server certificate to the certificate database by typing the appropriate command for the type of certificate:

- For a CA certificate, type

certutil -A -n *certificate_name* -d *certificate_directory* -i CA.cert -t C,C,C

- For a directory server certificate, type

certutil -A -n *certificate_name* -d *certificate_directory* -i *server_certificate.cert* -t P

where *certificate_name* is an alias that you assign, such as the CA name or host name; and *server_certificate* is the prefix of the directory server certificate file.

4. Copy the certificate database directory to the *c8_location*/configuration directory on every computer where Content Manager is installed.
5. Configure the directory server to use LDAPS and restart the directory server.
For more information, see the documentation for the directory server.
6. On the Content Manager computer where you configured the LDAP namespace to use the directory server, start IBM Cognos Configuration.
7. In the **Explorer** window, under **Security, Authentication**, click the LDAP namespace.
8. In the **Properties** window, for the **Host and port** property, change the port to the secure LDAPS port.
For the **SSL certificate database** property, specify the path to the cert7.db file.
9. In the **Explorer** window, right-click the LDAP namespace and click **Test**.
If the test fails, revise the properties, ensuring that the correct certificate is used.
10. From the **File** menu, click **Save**.
11. From the **Actions** menu, click **Restart**.
12. Repeat steps 6 to 11 on every other computer where Content Manager is installed.

Enabling Single Signon Between LDAP and IBM Cognos 8 Components

You achieve single signon to IBM Cognos 8 components by configuring the External Identity mapping property.

The External Identity mapping can refer to a CGI environment variable or an HTTP header variable. In the case of an application server gateway or dispatcher entry pointing to IBM Cognos 8 components, the External Identity mapping can refer to the userPrincipalName session variable. The resolved value of the External Identity mapping property at runtime must be a valid user DN.

When an LDAP namespace is configured to use the External Identity mapping property for authentication, the LDAP provider binds to the directory server using the Bind user DN and password or using anonymous if no value is specified. All users who log on to IBM Cognos 8 using external identity mapping see the same users, groups, and folders as the Bind user.

If you want IBM Cognos 8 components to work with applications that use Java or application server security, you can configure the External identity mapping property to obtain the user ID from the Java user principal. Include the token `${environment("USER_PRINCIPAL")}` in the value for the property. For more information, see the online help for IBM Cognos Configuration.

You can apply limited expression editing to the External Identity mapping property using the [replace operation](#).

Replace Operation

The replace operation returns a copy of the string with all occurrences of the old substring replaced by the new substring.

The following rules apply:

- The character `\` is used to escape the characters in the function parameters. Characters such as `\` and `"` need escaping.
- Nested function calls are not supported.
- Special characters are not supported.

Syntax

`${replace(str , old , new)}`

Parameter	Description
str	The string to search.
old	The substring to be replaced by the new substring.
new	The substring that replaces the old substring.

Examples

`${replace(${environment("REMOTE_USER")},"NAMERICA\\",)}`

`${replace(${environment("REMOTE_USER")},"NAMERICA\\", "")}`

Configuring IBM Cognos 8 Components to Use eTrust Site-Minder

To configure an authentication provider in an eTrust SiteMinder environment, you configure an LDAP, NTLM, or Netegrity SiteMinder namespace depending on your eTrust SiteMinder configur-

ation. Supported eTrust SiteMinder configurations are LDAP, Active Directory Server, and NTLM user directories.

Note: The authentication provider uses an eTrust SiteMinder SDK to implement a custom agent, and the custom agent deployment requires that the Agent Properties in the eTrust SiteMinder Policy server administration console be set to be able to support 4.x agents.

If eTrust SiteMinder is Configured For More Than One User Directory

If you configured eTrust SiteMinder for more than one user directory, you must use the Netegrity SiteMinder namespace. After configuring the Netegrity SiteMinder namespace in IBM Cognos 8, you must also add a corresponding LDAP, Active Directory Server, or NTLM namespace to the IBM Cognos configuration for each user directory defined in eTrust SiteMinder.

When configuring a corresponding LDAP namespace, you must ensure that the External identity mapping property is enabled and that you include the token REMOTE_USER in the value for the property. This does not mean that eTrust SiteMinder must be configured to set REMOTE_USER. The IBM Cognos Netegrity SiteMinder namespace passes user information internally to the corresponding LDAP namespace when it receives successful user identification from the eTrust SiteMinder environment.

When configuring a corresponding Active Directory namespace, you must ensure that the singleSignOnOption property is set to IdentityMapping. The IBM Cognos Netegrity SiteMinder namespace passes user information internally to the corresponding LDAP namespace using the REMOTE_USER environment variable when it receives successful user identification from the eTrust SiteMinder environment. For more information, see ["Enabling Single Signon Between Active Directory Server and IBM Cognos 8 Components" \(p. 153\)](#).

If eTrust SiteMinder is Configured With Only One User Directory

If eTrust SiteMinder is configured with only one user directory, the Netegrity SiteMinder namespace is not required. You can use the user directory as your authentication source by configuring the appropriate namespace, or you can configure the eTrust SiteMinder provider with one user directory. For example, if the eTrust SiteMinder user directory is NTML, you can configure IBM Cognos 8 components with an NTLM namespace or configure IBM Cognos 8 components with one Netegrity SiteMinder namespace, referring to one user directory that is an NTLM namespace.

If the eTrust SiteMinder user directory is Active Directory, you can use an Active Directory namespace or an LDAP namespace that is configured for use with Active Directory.

If you want to use the user directory as your authentication source directly instead of configuring a Netegrity SiteMinder namespace, configure the appropriate LDAP ([p. 161](#)), Active Directory ([p. 162](#)), or NTLM ([p. 178](#)) namespace. In this case, you must verify the Agent Configuration Object properties in eTrust SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

When configuring the LDAP namespace, in this case, you must ensure that the External identity mapping property is enabled and that you include the token REMOTE_USER in the value for the property.

When configuring the Active Directory namespace, in this case, you must ensure that the singleSignOnOption property is set to IdentityMapping. For more information, see ["Enabling Single Signon Between Active Directory Server and IBM Cognos 8 Components" \(p. 153\)](#).

To use an eTrust SiteMinder namespace and to set up single signon, do the following:

- ❑ [Configure IBM Cognos 8 components to use a Netegrity SiteMinder namespace](#)
- ❑ [Enable secure communication to the eTrust SiteMinder user directory](#), if required
- ❑ [Enable single signon between eTrust SiteMinder and IBM Cognos 8](#)
- ❑ [Protect the IBM Cognos Web alias](#).

You can hide the namespace from users during login ([p. 159](#)).

Configure a Netegrity SiteMinder Namespace

If you configured eTrust SiteMinder for more than one user directory, you must use the Netegrity SiteMinder namespace. After adding the Netegrity SiteMinder namespace, you must also add a corresponding LDAP or NTLM namespace for each user directory.

You can also configure an Netegrity SiteMinder namespace if users are stored in

- an LDAP server
- an NTLM server
- an Active Directory server

Steps

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the Netegrity SiteMinder namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.
7. In the **Explorer** window, under **Security, Authentication**, right-click the namespace and click **New resource, SiteMinder Policy Server**.
8. In the **Name** box, type a name for the policy server and click **OK**.
9. In the **Properties** window, specify the **Host** property and any other property values you want to change.

10. In the **Explorer** window, right-click the new SiteMinder Policy Server and click **New resource, User directory**.

Tip: Configure a user directory for each user directory in the SiteMinder policy server.

11. In the **Name** box, type a name for the user directory and click **OK**.

Important: The name of the user directory must match the name that appears on the policy server.

12. In the **Properties** window, type a value for the **Namespace ID reference** property.

13. From the **File** menu, click **Save**.

14. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

15. Configure a corresponding LDAP, Active Directory, or NTLM namespace for each LDAP, Active Directory, or NTLM user directory.

Important: Ensure that you use the same value for the **Namespace ID** property that you use for the **Namespace ID** property for the Netegrity SiteMinder namespace.

Enabling Secure Communication to the eTrust SiteMinder User Directory

If you use an SSL connection to the directory server, you must appropriately configure the IBM Cognos namespace for the user directory.

For more information, see ["Configure an LDAP Namespace" \(p. 161\)](#).

Enable Single Signon Between eTrust SiteMinder and IBM Cognos 8

By configuring single signon, you are not prompted to reenter authentication information.

IBM Cognos 8 components automatically refer to the eTrust SiteMinder session cookie for user session data.

If the eTrust SiteMinder user directory is LDAP or Active Directory, you must configure the eTrust SiteMinder user directory to use external identity mapping to the REMOTE_USER environment variable.

If the eTrust SiteMinder user directory is NTLM, Integrated Windows Authentication is used for single signon and no additional configuration is required.

Protecting the IBM Cognos Web Alias

eTrust SiteMinder must be configured correctly to protect the IBM Cognos Web alias.

Use the test tool provided with eTrust SiteMinder to verify that the resource is protected, authenticated, and authorized. For more information, see your eTrust SiteMinder documentation.

Hide the Namespace from Users During Login

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users login.

For example, you may want to integrate single signon across systems but maintain the ability for customers to authenticate directly to IBM Cognos 8 without being prompted to choose a namespace.

Steps

1. On each computer where you configured an eTrust SiteMinder authentication provider, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click the Netegrity Siteminder authentication provider.
3. In the **Properties** window, click the box next to **Selectable for authentication?** and then click **False**.
4. From the **File** menu, click **Save**.

The namespace is not shown on the selection list that is presented at login.

Configuring IBM Cognos 8 Components to Use an NTLM Namespace

You can configure IBM Cognos 8 components to use the Windows native security, NT LAN Manager (NTLM), as the authentication source.

If you are not using NTLM in your IS environment, you cannot use an NTLM namespace.

If you want to use an NTLM user directory as your authentication source with eTrust SiteMinder, you must verify the Agent Configuration Object properties in the eTrust SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

To use NTLM and to set up single signon, do the following:

- ☐ [configure an NTLM namespace](#)
- ☐ [enable single signon between NTLM and IBM Cognos 8 components](#)

Configure an NTLM Namespace

You can configure IBM Cognos 8 components to use an NTLM namespace when users are stored in an NTLM user directory. The NTLM user directory may also be accessed using an eTrust SiteMinder authentication provider.

Steps

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **NTLM** and click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.
Tip: Do not use colons (:) in the **NamespaceID** property.
6. Specify the values for all other required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.
7. From the **File** menu, click **Save**.
8. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Enable Single Signon Between NTLM and IBM Cognos 8 Components

By default, the IBM Cognos NTLM provider integrates with the IIS Web server for single signon if Windows integrated authentication (formerly named NT Challenge Response) is enabled on the IIS Web server.

If Windows integrated authentication is enabled, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the NTLM namespace.

Steps

1. Set up Windows integrated authentication on the IIS Web server.
2. Install Content Manager on a computer that is part of the domain, for the active and standby Content Manager computers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted for delegation.
4. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configuring IBM Cognos 8 to Use SAP

In SAP BW, you can assign users to user groups or roles or both. The SAP authentication provider uses only the roles.

The authorization rights required by the SAP user depend on who uses IBM Cognos 8 components, users or administrators.

SAP Authorization Settings for IBM Cognos 8 Users

The following authorization objects are required for any IBM Cognos user. Some of the values shown, such as *, are default values that you may want to modify for your environment.

Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	
	Name of RFC to be protected	RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO
	Type of RFC to be protected	FUGR
S_USER_GRP User Master Maintenance: User Groups	Activity	03
	Name of user group	*

SAP Authorization Settings for IBM Cognos Administrators

If users will perform administrative tasks and searches for users and roles, the following values must be added to the S_RFC authorization object in addition to the values listed above for IBM Cognos 8 users. Some of the values shown, such as *, are default values that you may want to modify for your environment.

Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	16
	RFC_NAME	PRGN_J2EE, SHSS, SOA3
	Type of RFC object to be protected	FUGR

To use SAP and to set up single signon, do the following:

- ☐ [Configure IBM Cognos 8 components to use an SAP namespace](#)
- ☐ [Enable single signon between SAP and IBM Cognos 8 components](#)

Configure an SAP Namespace

You can configure IBM Cognos 8 components to use an SAP server as the authentication source.

Steps

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **SAP** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all required properties to ensure that IBM Cognos 8 components can locate and use your existing authentication provider.

Depending on your environment, for the **Host** property, you may have to add the SAP router string to the SAP host name.

7. If the SAP system encodes the contents of cookies, enable the decode tickets feature:
 - In the **Properties** window, for **Advanced properties**, click the **Value** and then click the edit button.
 - Click **Add**.
 - Enter the name **URLDecodeTickets** and enter the value **true**
 - Click **OK**.

All SAP logon tickets will be decoded by the SAP namespace before establishing a connection.

8. From the **File** menu, click **Save**.
9. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Enable Single Signon Between SAP and IBM Cognos 8

You can enable single signon between SAP Enterprise Portal and IBM Cognos 8 components as well as when using the external namespace function of the SAP BW data source connections. To do so, ensure that you set the following system parameters on the SAP BW server:

- login/accept_sso2_ticket = 1
- login/create_sso2_ticket = 1

- `login/ticket_expiration_time = 200`

Test the Namespaces

After you configure one or more new namespaces for IBM Cognos 8 components, you can test the namespaces. The test can occur before or after you start the IBM Cognos 8 service. You can test all namespaces at the same time or test them individually.

Step to Test All Namespaces

- In the **Explorer** window, right-click **Authentication** and click **Test**.

IBM Cognos 8 components load, initialize, and configure the provider libraries for one namespace before testing the next namespace.

Tip: To cancel a namespace test, click **Cancel**. The test stops when the current namespace test is complete.

Step for a Single Namespace

- In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

IBM Cognos 8 components load, initialize, and configure the provider libraries for the namespace.

Delete an Authentication Provider

If they are no longer required, you can delete namespaces that you added or unconfigured namespaces that IBM Cognos 8 components detected.

Important: You must not delete the IBM Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration.

When you delete a namespace, you can no longer log on to the namespace. Security data for the namespace remains in Content Manager until you permanently delete it in the portal. For more information, see the *Administration and Security Guide*.

After you delete a namespace, it appears as Inactive in the portal.

Steps

1. On a computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, right-click the namespace and click **Delete**.

3. Click **Yes** to confirm.

The namespace disappears from the **Explorer** window and you can no longer log on to the namespace on that computer.

4. From the **File** menu, click **Save**.

5. Repeat steps 1 to 4 for each computer where you installed Content Manager.

You must now log on to the portal and permanently delete the data for the namespace. For more information, see the *Administration and Security Guide*.

Chapter 11: Configuring IBM Cognos 8 for an SAP Environment

IBM Cognos 8 Planning accesses SAP BW using the same OLAP interface as IBM Cognos 8 Business Intelligence components. However, to optimize performance for your planning applications, you can also create a detailed fact query subject in Framework Manager. This optimization allows a high volume of data for planning applications. The OLAP interface is optimized for reporting.

If your environment uses SAP components, you must configure it for IBM Cognos 8 to be able to access data or to administer users access.

Follow this process:

- ❑ [Verify the system requirements.](#)
- ❑ [Set access permissions](#) to model and run reports using SAP BW as a data source.

If you want to improve performance, [install IBM Cognos SAP gateway functions](#) and [set additional access permissions](#).

You can also use SAP components for authentication and as the application server running IBM Cognos 8 processes. For example, you can do the following:

- Enable single signon for Portal Services with the SAP logon ticket or with the user mapping.
- Enable secure communication between SAP EP and IBM Cognos 8 Components.
- Configure an SAP server as your authentication provider.

For more information about configuring SAP as an authentication source, see "[Configuring IBM Cognos 8 to Use SAP](#)" (p. 179).

Verify System Requirements

You must ensure that your environment meets the minimum requirements for IBM Cognos 8 components to use SAP as a data source.

Step

- Ensure that the following are installed on each IBM Cognos 8 server computer:
 - SAP GUI version 6.40 or later
 - BW Add-on

The BW Add-on is needed for SAP GUI to communicate with a BW server. It is selected when you install SAP GUI.

Set Access Permissions for Modeling and Reporting Access

For IBM Cognos products to be able to access SAP BW as a data source, the user accounts used to connect to SAP must have specific permissions. These permissions are required for the OLAP interface to SAP BW and are therefore relevant to both reporting and planning activities.

Incorrect permissions may result in run time errors. For more information, see ["Problems Creating a Module in Framework Manager Using a SAP BW Data Source" \(p. 237\)](#).

Step

- Ensure that the SAP accounts accessing the data source have the following permissions:

Authorization object	Field	Value
S_RFC	Activity	16 (Execute)
		RFC1
		RSAB
		RSOB
		RS_UNIFICATION
		RSNDI_SHIE
		RZX0
		SDTX
		SUGU
		SYST
S_TABU_DIS	RFC_TYPE	FUGR (Function Group)
	Activity	03 (Display)
		03 (Display)
S_RS_COMP	Authorization Group	&NC&
		SS
	Activity	03 (Display)
		16 (Execute)
	InfoArea	<i>All values</i>
	InfoCube	<i>All values</i>
	Name (ID) of reporting component	<i>All values</i>

Authorization object	Field	Value
S_RS_COMP1	Type of reporting component	<i>All values</i>
	Activity	03 (Display) 16 (Execute)
	Name (ID) of reporting component	<i>All values</i>
	Type of reporting component	<i>All values</i>
S_RS_HIER	Owner for	<i>All values</i>
	Activity	71 (Analyze)
	InfoObject	<i>All values</i>
	Hierarchy name	<i>All values</i>
S_RS_ICUBE	Hierarchy version	<i>All values</i>
	Activity	03 (Display)
	InfoCube Subobject	AGGREGATE DATA DEFINITION
	InfoArea	<i>All values</i>
	InfoCube	<i>All values</i>

Notes:

- *All values* indicates objects specific to your SAP environment to which you want to limit or permit access.
- &NC& represents any table that does not have an authorization group. For security reasons, create a new authorization group as a customization in the SAP BW system and assign the table RSHIEDIR to it. The new authorization group restricts the user's access to the previous table only, which is needed by Framework Manager.

Install and Configure IBM Cognos SAP Gateway Functions

To be able to create detailed fact query subjects in Framework Manager for Planning, you must install gateway function modules on your SAP server. You must also set additional permissions for the SAP account that will access the data.

The SAP gateway functions use Advanced Business Applications Programming (ABAP) function modules that interface with the SAP environment. The gateway functions must be installed on each SAP server that you want to use as a data source and should be installed by a SAP system administrator.

The module files are located in the *c8planning_location*\transports directory. A separate directory is created for each version of SAP that is supported.

If you are using SAP ERP Core Components versions ECC5 or ECC6, you must use the ABAP function modules in the *c8_location*\transports\v47 directory.

Steps for Windows

1. Copy the file named *Knn.ext* from the *c8_location*\transports\SAP_version directory to the *SAP_home*\trans\cofiles directory on the SAP server.
2. Copy the file named *Rnn.ext* from the *c8_location*\transports\SAP_version directory to the *SAP_home*\trans\data directory on the SAP server.

You can now apply the functions.

Step for UNIX

1. Copy the gateway functions from the Windows computer where you installed IBM Cognos 8 Planning to the UNIX computer where SAP is running.
2. Use file transfer protocol (FTP) in ASCII mode to copy the file named *Knn.ext* from the *c8_location*\transports\SAP_version directory to the *SAP_home*/trans/cofiles directory on the SAP server.
3. Use FTP in binary (bin) mode to copy the file named *Rnn.ext* from the *c8_location*\transports\SAP_version directory to the *SAP_home*/trans/data directory on the SAP server.

You can now apply the functions.

Apply the SAP Gateway Functions

After you install the SAP gateway functions, you must apply them using SAP GUI. Applying the functions should be performed by a SAP system administrator.

Steps

1. In the SAP GUI, start an STMS transaction.
2. Click **Imports**, and then double-click the queue name.
3. If a message appears prompting you to add to the import queue, click **Yes** and, if required, type your password.

4. In the queue, select the transport request name matching the name in the TRnames.txt file.
5. From the **Request** menu, click **Import** and type the target client number.
6. Click **Start Import**, and then click **Yes**. If required, type the password.
7. If you want to check the result, click **Logs**.

You can now install the IBM Cognos Compression Utility.

Install the IBM Cognos Compression Utility

The IBM Cognos compression utility is required for data compression on a SAP server. The corresponding decompression function is included in the SAP gateway functions.

Steps for Windows

1. Go to the *c8planning_location\bin* directory, and locate the files named *udacompr.exe* and *zlib1.dll*.
2. Copy these files to the *DIR_EXECUTABLE* directory on all Windows SAP servers.

The *DIR_EXECUTABLE* directory is usually defined as *SAP_instance\SYS\exe\run*.

Steps for UNIX

1. Using binary transfer mode, FTP the files from the *zipfiles\UNIX_platform* directory on the IBM Cognos 8 Planning Server CD to the *DIR_EXECUTABLE* directory on all UNIX SAP Servers.

The *DIR_EXECUTABLE* directory is usually defined as *SAP_instance/SYS/exe/run*.

2. Set execute privileges on each of the files.

Set Access Permissions for the IBM Cognos SAP Gateway Functions

For IBM Cognos SAP gateway functions to access SAP BW data, you must assign specific permissions to the user accounts that connect to the SAP server.

Incorrect permissions may result in run time errors. For more information, see ["Authorization Errors Using the IBM Cognos SAP Gateway"](#) (p. 239).

If your SAP security standards do not allow you to assign IBM Cognos 8 permissions for all files on your SAP server, you can restrict the directories to which the permissions apply. For more information, see ["Configuring a Logical Path to Manage SAP Temporary Files"](#) (p. 190).

Step

- Ensure that the SAP accounts accessing the data source have the following permissions:

Authorization object	Field	Value
S_RFC	Activity	16 (Execute)

Authorization object	Field	Value
S_BTCH_JOB	RFC_NAME	ZCOGNOS_80A
	Job Operations	RELE (Release Jobs)
	Job Group	RELE (Release Jobs)
S_DATASET	Activity	06 (Delete)
		33 (Read)
		34 (Write)
		A7 (Write with Filter)
	Physical file name	<i>All values</i>
	Program Name	<i>All values</i>

Notes

- *All values* indicates objects specific to your SAP environment to which you want to limit or permit access.
- S_DATASET must be assigned Delete permissions so that temporary files (.tmp) can be deleted. For more information, see ["Configuring a Logical Path to Manage SAP Temporary Files" \(p. 190\)](#).

Configuring a Logical Path to Manage SAP Temporary Files

By configuring a logical path on your SAP server, you can manage SAP temporary files without compromising the security standards of your SAP environment.

When IBM Cognos SAP gateway functions extract SAP data, they create temporary files (.tmp) on the SAP server. The operating system of the SAP server does not delete the .tmp files because it does not recognize them as temporary. The temporary files can grow very large unless an IBM Cognos function deletes them.

To allow the IBM Cognos SAP gateway functions to create and delete temporary files, you must assign Delete, Read, Write, and Write with Filter permissions to the S_DATASET object ([p. 189](#)). However, your SAP security standards may not allow you to apply these permissions for all files on your SAP server. You can restrict IBM Cognos 8 user permissions only to files in a specific directory. To specify this directory, you configure a logical path on your SAP server.

To configure a logical path, do the following:

- ☐ In your SAP application, call the transaction code FILE.
- ☐ Define a logical file path for IBM Cognos 8 temporary files.
- ☐ Assign a physical path, including the directory where temporary files will be stored, to the logical path that you defined previously.

- ❑ Define a logical file name that follows a predefined naming standard.

For more information, see your SAP documentation.

Chapter 12: Configuring Portal Services

Portal Services provides a set of Cognos portlets that you can use in IBM Cognos Connection and in other portals. You can use the portlets to navigate, search, and view IBM Cognos reports in your working environment. Other users can view IBM Cognos information without needing to know how to use IBM Cognos products.

For more information, see the *Administration and Security Guide*.

Portal Services is installed automatically with IBM Cognos 8 components. In a distributed environment, it is included with the Application Tier Components. The installation includes the deployment files for

- SAP Enterprise Portal (SAP EP)
- IBM WebSphere Portal
- BEA Aqualogic User Interface (ALUI) Portal
- SharePoint Portal

For some deployments of Portal Services, you must modify some Portal Services property settings and prepare the IBM Cognos environment to support the other portal.

When used in another portal, Portal Services can authenticate users in only one namespace. If IBM Cognos 8 components are configured with more than one namespace, you must install a separate gateway for each namespace that will be used to authenticate portal users. You must configure each gateway to use the appropriate namespace ([p. 126](#)) and then configure the deployed portlets to use that gateway.

After you configure the required properties, you must deploy the Cognos portlets to the other portal. For more information, see the *Administration and Security Guide*.

To use Portal Services with IBM Cognos 8 components, do the following:

- ❑ [Specify the location of the applications.xml file](#), if required.
- ❑ Install and test the portlets on the other portal.

For more information, see the *Administration and Security Guide*.

- ❑ [Configure security for the other portal environment](#).

Specify the Location of the Applications.xml File

If you use the applications.xml file as part of a custom application portlet, all Application Tier Components computers in a distributed environment must reference the same applications.xml file. If you have multiple instances of the applications.xml file, they must be identical.

Note: The steps are required only if you want to use the Extended Applications portlet, which is included with the IBM Cognos 8 software development kit.

Steps

1. On the computer where you installed the report server, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Portal Services**.
3. In the **Properties** window, click the **Value** next to **Location of 'applications.xml'**.
4. Replace localhost with a valid host name or IP address and, if necessary, replace the default port number.
5. From the **File** menu, click **Save**.

You can now deploy the Cognos portlets to your portal server. For instructions, see the *Administration and Security Guide*.

Configuring Security for Portal Services

When using Portal Services in another portal, you must enable single signon to provide seamless integration between the other portal and IBM Cognos 8 components.

Portal Services uses single signon to authenticate users. This means that users do not have to log on to other applications separately through the portal.

You must configure a URI into IBM Cognos 8 components for each portlet in Portal Services.

To enable security between IBM Cognos 8 components and the other portal, do the following:

- ☐ Disable anonymous access to IBM Cognos 8 components.

If your security infrastructure requires you to use another method for single signon, use one of the following methods:

- ☐ Enable single signon for the other portal using [shared secret](#).

If your security infrastructure requires you to use another method for single signon, use one of the following methods:

- ["Enable Single Signon for WebSphere Portal Using the Application Server"](#) (p. 202)
- ["Enable Single Signon for BEA ALUI Portal Using Basic Authentication"](#) (p. 202)
- ["Enable Single Signon for BEA ALUI Portal Using SiteMinder"](#) (p. 203)

- ☐ Configure IBM Cognos 8 components for SSL access, if required.

Disable Anonymous Access to IBM Cognos 8 Components

Portal Services uses single signon for authentication. If anonymous logon is enabled in IBM Cognos 8 components, Portal Services logs all portal users as anonymous. You must ensure that anonymous access is disabled in IBM Cognos 8 components for single signon in Portal Services to be successful.

However, you can test the Portal Services connections using anonymous logon to ensure that the portlets are working in the other portal.

If Portal Services fails to authenticate a user, the user receives an error message at the other portal.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, click **IBM Cognos**.
3. In the **Properties** window, ensure that **Allow anonymous access** is set to **False**.
4. From the **File** menu, click **Save**.
5. Repeat steps 1 to 4 on all servers where you installed IBM Cognos 8 components.

Enable Single Signon Using Shared Secret

You can use shared secret for single signon between Cognos portlets and IBM Cognos 8 components. The Cognos portlets send a message that contains an encrypted version of the portal user ID. The encryption key is determined by the value of a secret character string shared between the portlets and the custom Java security provider on the IBM Cognos server.

You can use shared secret for the other portal only if portal user IDs can be looked up in an NTLM, LDAP, or IBM Cognos Series 7 authentication namespace that is shared by IBM Cognos 8 components.

IBM Cognos 8 components must have access to a directory server that contains user IDs for all your portal users. Using IBM Cognos Configuration, you must configure an authentication namespace so that the portal and IBM Cognos 8 components share the same authentication source.

You must also create a Custom Java Provider namespace to register the shared secret Java provider that is provided with IBM Cognos 8 components. Within the portlets or iViews, you must link the portlets or iViews to the Custom Java Provider namespace within your respective portal:

- Cognos iViews (SAP EP)
- Cognos Portlet Application (WebSphere Portal)
- remote server (BEA ALUI Portal)
- Cognos WebPart (SharePoint Portal)

You are not required to configure access to the Portal Services Web content. However, if you deploy the portlets to another portal, you can configure access to an alternate URI for Portal Services images and Web content.

Steps to Configure the Required Namespaces

1. In IBM Cognos Configuration, configure a namespace to authenticate portal users.
For more information, see "[Configuring IBM Cognos 8 Components to Use an Authentication Provider](#)" (p. 147).
2. For an LDAP namespace, configure the following properties:

- For the **Use external identity** property, change the setting to **True**.
 - For the **External identity mapping** property, set it to
`{uid=${environment("REMOTE_USER")}}`
3. For an IBM Cognos Series 7 namespace, map the portal user IDs to IBM Cognos Series 7 user IDs using OS signons.
- For more information, see the IBM Cognos Series 7 documentation.
4. In IBM Cognos Configuration, create and configure a Custom Java Provider namespace.
- For the **Namespace ID** property, specify any new ID.
For example, **cpstrusted**
This new ID must be used in the portlet configuration settings.
 - For the **Java class name** property, type
com.cognos.cps.auth.CPSTrustedSignon
Java class names are case-sensitive.
5. In IBM Cognos Configuration, under **Environment, Portal Services**, configure the following properties:
- For **Trusted Signon Namespace ID**, type the namespace ID of the LDAP, NTLM, or IBM Cognos Series 7 namespace that you configured in step 1.
Tip: The trusted signon namespace acts as an intermediary and must be attached to a real directory-based namespace of type LDAP, NTLM, or IBM Cognos Series 7.
 - For **Shared Secret**, type the key to be used for single signon.
This parameter represents the authorization secret that must be shared between the Cognos portlets and the IBM Cognos server. Consider this as a secret password. You must use the same character string when you configure the portlet application. You must use a single word as the key.
For security reasons, we recommend you specify a non-null value.
6. Under **Environment**, for **Gateway Settings**, set the **Allow Namespace Override** property to **true**.
7. From the **File** menu, click **Save**.
8. Restart the IBM Cognos 8 service.

Steps to Configure Access to the Portal Services Web Content

1. On the computer where you installed the Application Tier Components, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Portal Services**.
3. In the **Properties** window, click the **Value** box next to **Web Content URI**.

4. Specify the host name or IP address of the gateway and a port number using the format *host_or_IP_address:port*
5. From the File menu, click **Save**.

Steps to Configure the Cognos iViews for SAP EP

1. Open the iView editor for each Cognos iView.
2. In the **Property Category** box, select **Show All**.
3. For the **cpsauthsecret: CPS Authorization Secret** property, enter the secret character string that you used for the Shared Secret property when you configured the Custom Java Provider namespace.
4. For the **cps: authentication namespace ID** property, enter the Custom Java Provider namespace ID.
5. For the **cpsserver: CPS Connection Server** property, enter the URL path to access Portal Services components through the gateway.

The format of the URL is as follows:

- For Cognos content portlets

Gateway_URI/wsrp/cps4/portlets/nav?wsdl&cb_action=cps.wsdl

Example for a CGI gateway:

http://myserver/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/nav?wsdl&cb_action=cps.wsdl

Example for a servlet gateway:

http://172.0.16.1:9500/wsrp/cps4/portlets/nav?wsdl&cb_action=cps.wsdl

- For Cognos Extended Applications

Gateway_URI/wsrp/cps4/portlets/sdk?wsdl&cb_action=cps.wsdl

Example for a CGI gateway:

http://myserver/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/sdk?wsdl&cb_action=cps.wsdl

Example for a servlet gateway:

http://172.0.16.1:9500/wsrp/cps4/portlets/sdk?wsdl&cb_action=cps.wsdl

- For Metrics Manager Watchlist portlets

Gateway_URI/wsrp/cps4/portlets/cmm?wsdl&cb_action=cps.wsdl

Example for a CGI gateway:

http://myserver/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/cmm?wsdl&cb_action=cps.wsdl

Example for a servlet gateway:

`http://172.0.16.1:9500/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl`

Steps to Configure the Cognos Portlets for WebSphere Portal

1. For each Cognos portlet application, click **Modify Parameters**.
2. For the **cps_auth_secret** property, enter the secret character string that you used for the **Shared Secret** property when you configured the Custom Java Provider namespace.
3. For the **cps_auth_namespace** property, enter the Custom Java Provider namespace ID.
4. For the **CPS Endpoint** property, enter the URL path to access Portal Services components through the gateway.

The format of the URL is as follows:

- For Cognos content portlets

Gateway_URI/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl

Example for a CGI gateway:

`http://myserver/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl`

Example for a servlet gateway:

`http://172.0.16.1:9500/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl`

- For Cognos Extended Applications

Gateway_URI/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

Example for a CGI gateway:

`http://myserver/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl`

Example for a servlet gateway:

`http://172.0.16.1:9500/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl`

- For Metrics Manager Watchlist portlets

Gateway_URI/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

Example for a CGI gateway:

`http://myserver/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl`

Example for a servlet gateway:

`http://172.0.16.1:9500/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl`

Steps to Configure the Remote Server for BEA Aqualogic User Interaction (BEA ALUI) Portal

1. Using a plain ASCII editor, such as Notepad, edit the `cpspt.properties` file in the `c8_location/cps/bea_aqualogic/webapps/gadgets/WEB-INF/classes` directory.

2. Configure the following settings.

Parameter	Value
cps_endpoint	<p>The URL to connect to the report server and extract the WSDL information.</p> <p>Specify the URI to the gateway.</p> <p>For a servlet or ISAPI gateway, replace the localhost/cognos8/cgi-bin/cognos.cgi portion with the values to target the gateway.</p> <p>For example,</p> <p>http://host_name/cognos8/cgi-bin/cognos.isapi/wsrp/cps4/portlets/[package]?wsdl&cb_action=cps.wsdl</p>
forward_cookies=	<p>The names of the cookie that should be sent to the report server for single signon.</p> <p>Leave blank.</p>
cps_auth_secret	<p>The shared secret code IBM Cognos 8 uses to encrypt an HTTP header variable that carries the user identity.</p> <p>This parameter represents the authorization secret that must be shared between the Cognos portlets and the IBM Cognos 8 server. Consider this as a secret password. Use the same value that you used for Shared Secret in IBM Cognos Configuration.</p> <p>For security reasons, we recommend you specify a non-null value.</p>
cps_auth_namespace	The namespace ID for the Custom Java Provider.

3. Go to the *c8_location/cps/bea_aqualogic* directory and run the following build file:

- On UNIX or Linux, **build.sh**
- On Windows, **build.bat**

This creates a cps-alui.war file in the *c8_location/cps/bea_aqualogic/gadgets* directory.

4. If IBM Cognos 8 components are running using Tomcat,

- Stop IBM Cognos 8.
- Copy the cps-alui.war file to the *c8_location/webapps* directory.
Tomcat automatically expands the WAR file and starts the remote server.
- Start IBM Cognos 8.

5. If IBM Cognos 8 components are running under another type of application server, copy the cps-alui.war file to the application server.

For instructions, see the administration guide for your application server.

Single signon is configured.

Steps to Configure Properties for the Cognos WebPart for SharePoint Portal

1. Using a plain ASCII editor, such as Notepad, edit the web.config file in the *drive*\Program Files\Common Files\Microsoft Shared\web server extensions\60\CONFIG directory.
2. Find the following string:

```
<SSO cps_auth_namespace="" cps_auth_secret="" />
```
3. Set cps_auth_namespace to the namespace ID for the Custom Java Provider namespace.
4. Set cps_auth_secret to the value that you used for **Shared Secret** in IBM Cognos Configuration.

Enable Single Signon for SAP EP with the SAP Logon Ticket

If you enable single signon with the SAP Logon Ticket, you must configure IBM Cognos 8 components with an SAP namespace that links to an SAP BW server.

Then you must copy the certificate that was generated during SAP EP installation to the SAP BW personal security environment.

Users must have the same user ID in all SAP systems that are accessed through single signon.

Before you start, ensure that you have

- configured IBM Cognos 8 components to use an SAP authentication source
- enabled single signon between IBM Cognos 8 components and SAP BW
- installed the latest service packs on the SAP BW server
Service packs can be downloaded from SAPNET.
- installed the latest hot patches for the SAP portal
- installed the Enterprise Portal plug-in that corresponds to the SAP EP release or SAP BW server
For SAP releases earlier than 6.2, on SAPNET, download EP50_PLUG-IN for Basis 620 (SAP-KINE32A). Using transaction SAINT, install SAPKINE32A.
- installed the SAP Security Library on the SAP BW servers
From sapservX, under /general/misc/security/SAPSECU/platform, download sapsecin and sepsecu.dll and place both files in the /run directory of the SAP BW server.

To enable SSO for SAP EP, complete the procedures for single signon with SAP logon tickets in the SAP Enterprise Portal *Security Guide*.

You can now use the Cognos iViews in the SAP Enterprise Portal. For more information, see the *Administration and Security Guide*.

Enable Single Signon for SAP EP with User Mapping

If you enable single signon with user mapping, you define an IBM Cognos data source in SAP EP. Individual users or an administrator can enter the user IDs and passwords for IBM Cognos 8 components in the data source. You must map the users logon credentials in the data source to an LDAP or IBM Cognos Series 7 or NTLM namespace. Portal Services iViews transmit the logon credentials to IBM Cognos 8 components using HTTP Basic Authentication.

Steps to Prepare the Environment

1. Configure the gateway URI that will be used by Portal Services to require authentication using HTTP Basic Authentication.

For information about configuring a URL to use HTTP Basic Authentication, see the documentation for the gateway or for your Web server.

2. Adjust the iView configuration to access the secure URL.
For information, see the documentation for your Web server.
3. In IBM Cognos Configuration, configure a namespace to authenticate portal users.
4. If you use an LDAP namespace, configure the following properties:
 - For the **Use external identity** property, change the setting to **True**.
 - For the **External identity mapping** property, set it to
`(uid=${environment("REMOTE_USER")})`

Steps to Create the Data Source and Map the Users

1. In the SAP portal, ensure that the following properties are configured for the data source in the `/PortalContent/other_vendors/every_user/com.cognos.pct.c8/systems/Cognos 8` directory:
 - **Logon Method** = UIDPW
 - **server name** = the name of the IBM Cognos server
 - **port number** = port number of the gateway
 - **Protocol of Target system** = HTTP
 - **User Mapping Type** = admin,user
 - **system alias** (Create a system alias)

For more information, see the SAP Enterprise Portal *Administration Guide*.

2. For each Cognos iView, enable user mapping for the data source by entering the name of the system alias at the iView level, in an attribute called **CPS: User Mapping Datasource**.

For more information, see the SAP Enterprise Portal *Administration Guide*.

3. For each Cognos iView, set the **CPS: Authentication Namespace ID** property to the namespace that you want to use for authentication.

4. Register the IBM Cognos credentials for the portal users.

Users can enter their own user IDs and passwords.

For more information, see the SAP Enterprise Portal *Administration Guide*.

We recommend that you enable secure communication between SAP EP and IBM Cognos 8.

You can now use the Cognos iViews in the SAP Enterprise Portal. For more information, see the *Administration and Security Guide*.

Enable Secure Communication Between SAP EP and IBM Cognos 8 Components

A secure connection, using SSL, is not required between SAP EP and IBM Cognos 8 components. It is more important if you enabled single signon with user mapping.

The SSL security supported by SAP uses encryption above 56 bits. By default, IBM Cognos 8 components use an encryption algorithm up to 56 bits. IBM Cognos provides an enhanced encryption module as a complementary product. To enable SSL, you must purchase and install the Enhanced Encryption Module for OpenSSL on top of IBM Cognos 8 components. For more information, see the IBM Cognos Enhanced Encryption Module for OpenSSL *Installation and Configuration Guide*.

To enable SSL between SAP EP and IBM Cognos 8 components, see your SAP EP security documentation.

After SSL is enabled, edit properties for the all iViews so that the **cpsserver: CPS Connection Server** property uses https instead of http.

You can now use the Cognos portlets in the SAP Enterprise Portal. For more information, see the *Administration and Security Guide*.

Enable Single Signon for WebSphere Portal Using the Application Server

The Portal Services portlets can use the Active Credentials objects provided by WebSphere Portal to connect to IBM Cognos 8 components. Portal Services supports the following Active Credentials objects: HttpBasicAuth, LtpaToken, SiteMinderToken, and WebSealToken.

Credentials for the portal user are passed to the gateway using this object. For more information about Active Credential objects, see the documentation for IBM WebSphere Portal.

To use application server single signon, see the documentation for IBM WebSphere Application Server.

After single signon is set up, you can use the Cognos portlets in the WebSphere Portal. For more information, see the *Administration and Security Guide*.

Enable Single Signon for BEA ALUI Portal Using Basic Authentication

You can configure a portlet in BEA ALUI Portal to send the username and password as an HTTP Basic authentication header. The header can be used with an NTLM, LDAP, or IBM Cognos Series 7 authentication namespace to provide single signon.

Steps

1. In IBM Cognos Configuration, configure a namespace to authenticate portal users.

2. Install an alternate CGI or ISAPI or servlet gateway in IBM Cognos 8.
3. Configure the gateway.
4. In the administration console of the Web server, configure the virtual directories to access the gateway.

For more information, see the documentation for your Web server.

5. Configure the BEA ALUI remote server to access IBM Cognos 8:
 - Edit the `cpspt.properties` file in the `c8_location/cps/bea_aqualogic/webapps/gadgets/WEB-INF/classes` directory.
 - Change the `cps_endpoint` property to indicate the URL of the gateway.
 For a CGI gateway, you can use the default setting if the gateway and the remote server are on the same computer. Otherwise, replace the `localhost` portion with **`host_name:port`**
 For a servlet or ISAPI gateway, replace the `localhost/cognos8/cgi-bin/cognos.cgi` portion with the values to target the gateway.
 For example,
`http://host_name:port/cognos8/cgi-bin/cognos.isapi/wsrp/cps4/portlets/[package]?wsdl&cb_action=cps.wsdl`
 - Set the `cps_auth_namespace` property to the namespace that you want to use for authentication.

Enable Single Signon for BEA ALUI Portal Using SiteMinder

If you use eTrust SiteMinder to provide single signon in your security infrastructure, you can also use it for single signon with BEA ALUI Portal.

You must configure a SiteMinder authentication namespace in IBM Cognos 8. BEA ALUI Portal sends the SiteMinder active authentication token to the remote server, which sends the token to the IBM Cognos 8 gateway.

Steps

1. In IBM Cognos Configuration, configure a SiteMinder authentication namespace.
 For instructions, see ["Configuring IBM Cognos 8 Components to Use eTrust SiteMinder"](#) (p. 174).
2. Configure the remote server to forward the authentication token:
 - Edit the `cpspt.properties` file in the `c8_location/cps/bea_aqualogic/webapps/gadgets/WEB-INF/classes` directory.
 - Change the `forward_cookies` property to include the name of the active authentication token that SiteMinder provides.
 - Change the `cps_endpoint` property to indicate the URL of the gateway.
 For a CGI gateway, you can use the default setting if the gateway and the remote server are on the same computer. Otherwise, replace the `localhost` portion with **`host_name:port`**.

For a servlet or ISAPI gateway, replace the `localhost/cognos8/cgi-bin/cognos.cgi` portion with the values to target the gateway.

For example,

`http://host_name:port/cognos8/cgi-bin/cognos.isapi/wsrp/cps4/portlets/[package]?wsdl&cb_action=cps.wsdl`

- Change the `cps_auth_namespace` property to the namespace that you want to use for authentication.

Chapter 13: Setting Up an Unattended Installation and Configuration

Set up an unattended installation and configuration to

- install an identical configuration across several computers on your network
- automate the installation and configuration process by specifying options and settings for users

Before you set up an unattended installation and configuration, ensure that all the system requirements and prerequisites are met and that all third-party products are installed and configured.

To set up an unattended installation and configuration:

- ☐ configure a transfer specification file (.ats) to specify installation options
- ☐ run the installation tool in silent mode
- ☐ use a preconfigured configuration file from another computer
- ☐ run the configuration tool in silent mode

After you complete these tasks, ensure that the IBM Cognos 8 Planning installation directory on all computers is protected from unauthorized or inappropriate access.

Set Up an Unattended Installation

Use a transfer specification file (.ats) to copy IBM Cognos 8 Planning components, including Analyst, to your computer without being prompted for information.

By default, each time you install IBM Cognos 8 Planning components using the installation wizard, the options you select are recorded in a transfer specification file. Therefore, if you already installed IBM Cognos 8 Planning components on a sample computer, you can use the generated transfer specification file as a template for unattended installations on different computers.

If you do not use the installation wizard to install components, you can use the default transfer specification file named `response.ats` that is available on the CD. You must modify the `response.ats` file for your environment before you can use it for an unattended installation.

You can check if the unattended installation was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.

Steps Using a File Generated by a Previous Installation

1. Use the installation wizard to install IBM Cognos 8 Planning components on your computer.
2. Go to `c8Planning_location\instlog`.
3. Locate the transfer specification file (.ats) that was generated:

- If you installed IBM Cognos 8 Planning - Server, the file name is *ts-PLANSRVR-version-yyyymmdd_bhmm.ats*.
 - If you installed IBM Cognos 8 Planning - Administration, the file name is *ts-PLANADMIN-version-yyyymmdd_bhmm.ats*.
 - If you installed IBM Cognos 8 Planning - Client, the file name is *ts-PLANCLIENT-version-yyyymmdd_bhmm.ats*.
4. Copy the transfer specification file to the computer where you plan to install IBM Cognos 8 Planning.
 5. On the computer where you plan to install the software, insert the appropriate CD and copy the contents of the CD to your computer.
 6. Install IBM Cognos 8 Planning:
 - On Windows, open a **Command Prompt** window, and change to the win32 directory where you copied the contents of the CD, and then type the following command, where *location* is the directory where you copied *filename*, the transfer specification file:

issetup -s location/filename.ats

If zero (0) is not returned, check the log files for error messages. Errors are recorded in the installation directory in the following log file:

- For IBM Cognos 8 Planning - Server the file name is *tl-PLANSRVR-version-yyyymmdd-bhmm_summary-error.txt*.
- For IBM Cognos 8 Planning - Administration, the file name is *tl-PLANADMIN-version-yyyymmdd-bhmm_summary-error.txt*.
- For IBM Cognos 8 Planning - Client the file name is *tl-PLANCLIENT-version-yyyymmdd-bhmm_summary-error.txt*.

If errors occur before sufficient initialization occurs, log messages are sent to one of the following log files in the Temp directory:

- For IBM Cognos 8 Planning - Server, the file name is *tl-PLANSRVR-version-yyyymmdd-bhmm.txt*.
- For IBM Cognos 8 Planning - Administration, the file name is *tl-PLANADMIN-version-yyyymmdd-bhmm.txt*.
- For IBM Cognos 8 Planning - Client the file name is *tl-PLANCLIENT-version-yyyymmdd-bhmm_summary-error.txt*.

Also ensure that the installation directory is protected from unauthorized or inappropriate access.

After all errors are resolved, you can [set up an unattended configuration](#).

Steps Using the Response.ats File

1. On the target computer, insert the CD and copy the contents to your computer.

2. Go to the win32 directory and open the response.ats file in a text editor.
Each section in the response.ats file corresponds to a dialog box in the installation wizard.
3. Type the installation location of the program files for IBM Cognos 8 Planning in APPDIR=*location*.
Tip: There should be no space on either side of the equal sign, (=).
4. For the server components of IBM Cognos 8 Planning, in the section named [Component List], next to each component:
 - To install the component, type 1
 - To not install the component, type 0**Note:** You do not select components for Analyst. All required files are installed.
5. For a Windows installation, for the APPFOLDER= property, type the name of the **Start** menu folder that contains your program shortcuts.
Tip: To ensure that the shortcut folder is visible to all users, type 1 for the ALLUSERS_FLAG= property.
6. For the install information in the [Install Conditions] section:
 - To specify that the condition is true, type 1
 - To specify that the condition is false, type 0
7. Save the response.ats file to a local directory after you make the necessary changes.
8. Go to the win32 directory.
9. At the command prompt type the following command, where location is the directory where you copied response.ats:
 - Type
issetup -s *location*/response.ats

If zero (0) is not returned, check the log files for error messages. Errors are recorded in the installation directory in the following log file:

- For IBM Cognos 8 Planning - Server the file name is tl-PLANSRVR-*version-yyyy-mm-dd-hhmm*_summary-error.txt.
- For IBM Cognos 8 Planning - Administration, the file name is tl-PLANADMIN-*version-yyyy-mm-dd-hhmm*_summary-error.txt.
- For IBM Cognos 8 Planning - Client the file name is tl-PLANCLIENT-*version-yyyy-mm-dd-hhmm*_summary-error.txt.

If errors occur before sufficient initialization occurs, log messages are sent to one of the following log files in the Temp directory:

- For IBM Cognos 8 Planning - Server, the file name is tl-PLANSRVR-*version-yyyy-mm-dd-hhmm*.txt.

- For IBM Cognos 8 Planning - Administration, the file name is `tl-PLANADMIN-version-yyyyymmdd-hhmm.txt`.
- For IBM Cognos 8 Planning - Client the file name is `tl-PLANCLIENT-version-yyyyymmdd-hhmm_summary-error.txt`.

Also ensure that the installation directory is protected from unauthorized or inappropriate access.

After all errors are resolved, you can set up an unattended configuration.

Set Up an Unattended Configuration

Before you set up an unattended configuration, you must export a configuration from another computer that has the same IBM Cognos 8 Planning components installed. You can then run IBM Cognos Configuration in silent mode.

The exported configuration contains the properties of the IBM Cognos 8 Planning components that you installed on the source computer. If you made changes to the global configuration, you must also copy the global configuration file from the source computer to the computer where you plan to run an unattended configuration.

Ensure that the configuration settings on the local computer are appropriate to use to configure another IBM Cognos 8 Planning computer with the same installed components. For example, if you changed the host name portion of the Gateway URI property from local host to an IP address or computer name, ensure this setting is appropriate for the new computer's configuration.

You can check if the unattended configuration was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.

Steps

1. In IBM Cognos Configuration, from the **File** menu, click **Export as**.
2. If you want to export the current configuration to a different folder, in the **Look in** box, locate and open the folder.
Ensure that the folder is protected from unauthorized or inappropriate access.
3. In the **File name** box, type a name for the configuration file.
4. Click **Save**.
5. Copy the exported configuration file from the source computer or network location to the `c8_location/configuration` directory on the computer where you plan to do an unattended configuration.
6. Rename the file to `cogstartup.xml`.
7. If you changed the global configuration on the source computer, copy the `coglocale.xml` file from the source computer to the `c8planning_location/configuration` directory on the computer where you plan to do an unattended configuration.
8. Go to `c8planning_location/bin`.

9. Type the configuration command:

- Type
cogconfig.bat -s

Tip: To view log messages that were generated during an unattended configuration, see the `cogconfig_response.csv` file in the *c8planning_location/logs* directory.

IBM Cognos Configuration applies the configuration settings specified in the local copy of `cogstartup.xml`, encrypts credentials, generates digital certificates, and if applicable, starts the IBM Cognos 8 service or process.

Chapter 14: Setting Up the Samples for Contributor

The IBM Cognos 8 Planning installation includes both Analyst and Contributor samples to help you get started using the product. These samples are installed in the *C8planning_location\samples\Planning* directory.

The Analyst samples require no further setup if an Analyst user wants to access the samples in the language that you selected when you installed IBM Cognos 8 Planning - Server or IBM Cognos 8 Planning - Administration. However, if an Analyst user wants to access the samples in a different language than the one you selected during installation, you must change the language of the samples. For more information, see ["Change the Language of the Analyst Samples" \(p. 105\)](#).

The Contributor samples must be configured before they can be used in IBM Cognos 8 Planning - Contributor. Use this checklist to set up the go_contributor samples. Detailed information follows for each of these tasks:

- ☐ [Install Sun Java Systems directory server.](#)
- ☐ [Import the authentication data from Contributor_sample.ldif to a Sun Java Systems directory server.](#)
- ☐ [Configure IBM Cognos 8 Planning to use your Sun Java System directory server.](#)
- ☐ [Configure Contributor Administration.](#)
- ☐ [Create the Contributor applications.](#)

Install Sun Java Systems Directory Server

The sample authentication data is provided in a format used by the Sun Java System Directory Server. You must install the directory server before you can import the authentication data to use the IBM Cognos 8 Planning samples.

When you create the directory server for the sample authentication data, ensure that the **Base Suffix** value or base domain is **dc=grtd123,dc=com**. This is the domain used in the sample authentication data.

You can download the Sun Java System Directory Server from the Sun Website (www.sun.com). For instructions about installing the directory server, see the product documentation.

Import the Sample Authentication Data

The authentication data used for the IBM Cognos 8 Planning samples is provided in LDAP data interchange format (LDIF). To use the authentication data you must import it into a Sun Java System Directory Server.

The LDIF file provided with the Contributor samples is named `Contributor_sample.ldif`, and is located in the `C8_location\samples\Planning\Contributor\language\Data` directory.

Steps

1. Open the Sun ONE Server Console.
2. Click the **Servers and Applications** tab, expand the tree and click the directory server instance into which you want to import the sample authentication data.
Ensure that the **Base Suffix** value or base domain is `dc=grtd123,dc=com` for the directory server.
3. In the right pane of the window, click **Open**.
4. On the **Tasks** tab, click **Import from LDIF**.
5. In the **Import LDIF** box, enter the location of the `Contributor_sample.ldif` file.
6. Select **Continue on error**.
7. In the **File for rejects** box, enter the location and file name for your error log.
8. Click **OK**.

You should receive error messages indicating that two objects already exist. These are default objects in the Sun Java System Directory Server.

If no objects are imported, ensure that the **Base Suffix** value or base domain is `dc=grtd123,dc=com` for the directory server and that you have selected **Continue on error** before you re-import the authentication data.

Configure IBM Cognos 8 Planning to Use Your Sun Java System Directory Server

To use IBM Cognos 8 Planning you must configure your Sun Java System Directory Server as an authentication source and you must disable anonymous access for users.

If you have installed IBM Cognos 8 Planning components on different computers, you must configure the directory server information on the computer where Content Manager is installed.

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security, Authentication**, click **IBM Cognos**.
3. In the **Properties** window, ensure that **Allow anonymous access** is set to **False**.
4. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New Resource, Namespace**.
5. Type a **Name**, and click **LDAP** in the **Type** box.
6. In the **Resource Properties** window, enter the following information:

- In **Namespace ID**, type a name for the samples namespace. The name can be anything you choose.
 - In **Host and Port**, enter the computer name and port number for your Sun Java System Directory Server.
 - In **Base Distinguished Name**, type the following:
dc=grtd123,dc=com
 - In **User Lookup**, type the following:
(uid=\${userID})
7. From the **File** menu, click **Save**.
 8. In the **Explorer** window, click **Local Configuration**.
 9. From the **File** menu, click **Action, Restart**.

Configure Contributor Administration

If you are opening Contributor Administration for the first time, you must create the planning tables in the planning store and add a planning datastore server.

For instructions about configuring the Contributor Administration, see the Contributor *Administration Guide*.

GO Contributor Sample

The GO Contributor sample consists of applications that can be linked together. These applications are named `go_capex_contributor`, `go_personnel_contributor`, and `go_expenses_contributor`. A flowchart is provided in IBM Cognos 8 Planning - Manager in the `go_expenses_contributor` library. Each application uses its own e.list, which is typical in a planning environment.

Library	e.List	Type
<code>go_capex_contributor</code>	2 Divisions (elist)	Depreciation
<code>go_personnel_contributor</code>	2 EList (Departments)	Payroll
<code>go_expenses_contributor</code>	2 EList (Departments)	Expenses

D-Lists and formats used by the libraries in the table above are stored in the `go_common_contributor` library.

The `go_capex_contributor` Application

The `go_capex_contributor` application is designed to capture details of planned capital purchases and calculate the depreciation charge on those items. This depreciation is then added to the depre-

ciation on the existing items that is imported from external systems to determine the total depreciation charge. The application consists of the following cubes.

- **Asset Purchases**
This cube captures the description, asset type, value, target department, and month of purchase by version. There is also an item that highlights any invalid target department.
- **Depreciation**
This cube calculates the depreciation to be charged to each department.
- **Depn Policy**
This cube holds the life and depreciation charge for each type of asset. It is provided only for information purposes and users cannot change the data in this cube. Because it does not have an e.List dimension, this cube is known as an assumption cube. Data for assumption cubes must be input in Analyst and moved into Contributor by synchronizing the application and performing Go to Production.
- **Valid Departments**
Because not all departments operate in the same geographic region, only valid target departments may be entered in Asset Purchases. This cube shows which departments are valid for the division.

The following table provides information about the go_capex_contributor data files.

Operation in console	Data file name
e.List	Capex_Elist.txt
Rights	capex_rights.txt
User Classes	capex_rights.txt
Access Tables	Access_Valid Departments.txt Access_Validity check.txt Access_Actual.txt Access_Yes.txt
Help Text	Simple_Help.txt Capex_Detailed_Help.txt
Administration Links	Go_depreciation.cal
Data	Depreciation.txt Asset purchases.txt Valid departments.txt

The go_personnel_contributor Application

The go_personnel_contributor application is designed to capture payroll-related items and to ensure the required levels of separation of responsibilities. The data is then fed into the go_expenses_contributor application. Viewing cubes is controlled by access tables. The application consists of the following cubes:

- Salaries

This cube captures each employee's grade, percent raise, and month raise if applicable. The base salary is determined from the Salary by Grade cube based on the selected grade. The monthly salary is calculated to include the base and the raise. If the month that the raise is to be applicable is missing, a warning message appears. An access table is available for this cube to ensure that employees are visible only in the correct departments.

- Benefits

This cube determines additional employee costs by country and version. The appropriate benefit percentages are applied by country.

- Salary by Grade and Band

Because it does not have an e.List dimension, this cube is known as an assumption cube that holds Salaries by Grade and Band by Country.

We recommend that this cube be hidden.

- Benefit %s

This is an assumption cube that holds benefit percentages by Country. The benefit percent data is not necessarily indicative of current rates.

We recommend that this cube be hidden.

The following table provides information about the go_personnel_contributor data files.

Operation in console	Data file name
e.List	Personnel_elist.txt
Rights	Personnel_rights.txt
User Classes	Personnel_rights.txt
Access Tables	Access_Table_Salaries.txt
	Access_Table_Employees.txt
	Access_Table_Benefits.txt
	Access_Table_Countries.txt
	Access_Table_Versions.txt
Administration Links	Go_personnel.cal

Operation in console	Data file name
Data	Salaries.txt
	Salaries_Band_Grade.txt
	Benefits.txt

The go_expenses_contributor Application

The go_expenses_contributor application is designed to capture expenses and create an expense summary. The application consists of the following cubes.

- **Travel Costs**
Users are asked to consider their travel plans in terms that they understand. Rather than just providing an amount for the key expenditure items, they are asked to provide lower-level details that are likely to be more relevant to them, such as hotel cost per night.
- **Comm Costs**
Users are asked to consider communication costs at a lower level of detail, including number of lines, handsets, and terminal blocks.
- **Supply Costs**
Users are asked to input an amount for expenditure items at a high level, such as computer costs and office costs.
- **Marketing**
This cube is the subject of an access table, which means that it is available only to the Marketing department. All other departments do not see this cube. Users are asked to consider their marketing plans in terms that they understand. Rather than just providing an amount for the key expenditure items, they are asked to provide lower-level details which are likely to be more relevant to them.
- **Corporate Expenses**
This cube summarizes all the detail that was captured by the other cubes and captures expense items that do not require greater detail. Information also comes from the go_capex_contributor and go_personnel_contributor applications.

The following table provides information about the go_expenses_contributor data files.

Operation in console	Data file name
e.List	Expenses_Elist.txt
Rights	Expenses_rights.txt
User Classes	Expenses_rights.txt

Operation in console	Data file name
Access Tables	Access_Actual.txt
	Access_Depreciation.txt
	Access_Marketing.txt
	Access_Divisions.txt
	Access_Countries.txt
Data	Communications.txt
	Supplies.txt
	Travel.txt
	Corporate expenses.txt

Create Contributor Applications

When importing data, ensure that the database code page parameter reflects the underlying data being imported.

For example, when you are importing non-Western European language data or data containing non-ASCII characters, you must set the **Import Options** parameter to -C1252 (the Microsoft Windows default code page) for the import load routine to complete successfully.

For more information about using Contributor Administration, see the *Contributor Administration Guide*.

The data files are stored in the *c8_location*\samples\Planning\Contributor\language\Data directory.

Steps

1. In Contributor Administration, specify the application ID that was set for each sample application, as follows:
 - application ID for go_capex_contributor: 90040011
 - application ID for go_expenses_contributor: 90040012
 - application ID for go_personnel_contributor: 90040014

Otherwise, when you import the sample administration links, you are prompted to reselect the source and target applications.

2. For each application, do the following:
 - Import the e.List and rights text files.
 - Set Navigation (optional).
 - Set Orientation (optional).
 - Import access tables (optional).

- Make appropriate cubes hidden or read only (optional).
- Run Go to Production.

Tip: You do not need to use cut-down models.

3. Import administration links.

Steps to Set the Import Options Parameter

1. In Contributor Administration, expand **Datastores**, *data store name*, **Applications**, *application name*, **Development**, **Application Maintenance**, and click **Admin Options**.
2. In **Import Options**, enter the parameter value.

If you are importing non-Western European language data or data containing non-ASCII characters, enter -C1252.

Recommended Cube Settings

The following settings are recommended to each of the sample cubes. You apply the settings in Contributor Administration.

The go_capex_contributor Cube

For the go_capex_contributor cube, the following settings are recommended.

Web-Client Configuration

The recommended **Navigation** and **Orientation** settings are shown in the table below:

Cube	Pages	Rows	Columns
Asset purchases	2 Divisions (elist) 5 Versions	3 ID number	1 Asset purchases
Depreciation	2 Divisions (elist) 1 Depreciation 2 Departments 5 Versions	2 Asset types	4 Months
Depreciation Policy	N/A	2 Asset types	3 Depn policy
Valid departments	N/A	3 Departments (Yes)	2 Divisions (elist)

Other settings include:

- For **Grid Options**, use the default settings.
- For the **Application Options**, use the default settings.

It may be appropriate to allow **Reviewer Edit** and **Bouncing**.

- Clear the **Planner Only Cubes** options.
- For the **Contributor Help Text** options, two files are provided. The text in Simple_help.txt can be copied into the **Simple Cube Help** box. The html code in Capex_detailed_help.txt can be copied into the **Detailed Cube Help** box.

Application Maintenance

The recommended settings for **Application Maintenance** include:

- For **Admin Options**, select **Yes** for **Act As System Link Source**.
- For **Go To Production Options**, use the default settings.

Access Tables and Selections

The following **Access Tables** are provided:

File Name	Dimensions	Cubes	eList?	Reason
Access_ Valid Departments .txt	2 Departments	Depreciation	Yes	Restricts the departments visible to users to those valid in their country.
Access_ Validity check.txt	1 Asset Purchases	Asset Purchases	No	Hides the data used for the validity check.
Access_ Actual.txt	5 Versions	Depreciation Asset Purchases	No	Ensures actual data is read only
Access_ Yes.txt	3 Departments (Yes)	Valid Depart- ments	No	Hides Total item

Note that cut down models were not used, but hide functionality was used extensively.

The following are cubes without access tables:

Cube	Access Level
Assumption Cube	Depn Policy
	Read

The go_expenses_contributor Cube

For the go_expenses_contributor cube, the following settings are recommended.

Web-Client Configuration

The recommended **Navigation** and **Orientation** settings are shown in the table below:

Cube	Pages	Rows	Columns
Travel Costs	2 Elist (Departments) 2 Divisions 5 Versions	1 Travel Costs	4 Months
Supply Costs	2 Elist (Departments) 2 Divisions 5 Versions	1 Supply Cost	4 Months
Comm Costs	2 Elist (Departments) 2 Divisions 5 Versions	1 Comm Costs	4 Months
Marketing	2 Elist (Departments) 2 Campaigns 2 Divisions 5 Versions	1 Marketing	4 Months
Corporate Expenses	2 Elist (Departments) 2 Divisions 5 Versions	1 Accounts	4 Months

Other settings include:

- For **Grid Options**, use the default settings.
- For the **Application Options**, use the default settings.
It may be appropriate to allow **Reviewer Edit** and **Bouncing**.
- Clear the **Planner Only Cubes** options.
- For the **Contributor Help Text** options, use the default settings.

Application Maintenance

The recommended settings for **Application Maintenance** include:

- For **Admin Options**, use the default settings.
- For **Go To Production Options**, use the default settings.

Access Tables and Selections

The following **Access Tables** are provided:

File Name	Dimension	Cube	eList?	Reason
Access_ actual.txt	5 Versions	Corporate Expenses Marketing Travel Costs	No	Ensures that the actual data is read only
Access_ depreci- ation .txt	1 Accounts	Corporate Expenses	No	Ensures that the Depreciation amount imported from capex application cannot be overwritten
Access_ marketing .txt	1 Marketing	Marketing	Yes	Ensures that the Marketing tab is hidden from all but the Marketing department
Access_ divis- ions.txt	2 Divisions	Corporate Expenses Marketing Travel Costs	Yes	Allows write access to the correct departments by division

Note that cut down models were not used, but hide functionality was used extensively.

The go_personnel_contributor Cube

For the go_personnel_contributor cube, the following settings are recommended.

Web-Client Configuration

The recommended **Navigation** and **Orientation** settings are shown in the table below:

Cube	Pages	Rows	Columns
Salaries	2 Elist (Departments)	2 Employees	1 Salaries
Benefits	2 Elist (Departments) 3 Countries 5 Versions	1 Benefits	4 Months
Salary by Grade and Band	2 Bands	3 Countries	3 Grades
Benefit %s	N/A	3 Countries	3 Benefit %s

Other settings include:

- For **Grid Options**, use the default settings.
- For the **Application Options**, use the default settings.

It may be appropriate to allow **Reviewer Edit** and **Bouncing**.

- Clear the **Planner Only Cubes** options.
- For the **Contributor Help Text** options, use the default settings.

Application Maintenance

The recommended settings for **Application Maintenance** include:

- For **Admin Options**, use the default settings.
- For **Go To Production Options**, use the default settings.

Access Tables and Selections

The following **Access Tables** are provided:

File Name	Dimension	Cube	eList?	Reason
Access_Table_ 1 Salaries Salaries.txt	1 Salaries	Salaries	No	Ensures appropriate data entry
Access_Table_ 2 Employees Employees .txt	2 Employees	Salaries	Yes	Allows employees to be visible in the correct departments
Access_Table_ 1 Benefits Benefits.txt	1 Benefits	Benefits	No	Ensures appropriate data entry
Access_Table_ 3 Countries Countries.txt	3 Countries	Benefits	Yes	Allows write access to the correct departments by country
Access_Table_ 5 Versions Versions.txt	5 Versions	Benefits	No	Ensures that the actual data is read only

Note that cut down models were not used, but hide functionality was used extensively.

The following are cubes without access tables:

	Cube	Access Level
Assumption	Salary by grade	Hidden
Assumption	Benefit %s	Hidden

Chapter 15: Troubleshooting

Use the troubleshooting reference information and solutions as a resource to help you solve specific problems you may encounter during or after the installation of IBM Cognos 8 components.

For more information about troubleshooting resources, see the *Troubleshooting Guide*.

Problems are characterized by their symptoms. Each symptom can be traced to one or more causes by using specific troubleshooting tools and techniques. After being identified, each problem can be fixed by implementing a series of actions.

When you are troubleshooting, log files can help you. Another valuable troubleshooting tool is the Knowledge Base, which is available on the Cognos Software Services Web site (<http://support.cognos.com>). The Knowledge Base is a database of problems and solutions for all IBM Cognos products.

When you cannot resolve a problem, the final resource is your technical support representative. To analyze a problem, your technical support representative requires information about the situation and the symptoms that you are experiencing. To help isolate the problem, collect the necessary data before you contact your representative.

Log Files

Log files can help you troubleshoot problems by recording the activities that take place when you work with a product. Operations performed in IBM Cognos 8 are recorded in various log files for tracking purposes. For example, if you experienced problems installing IBM Cognos 8, consult the transfer log file to learn what activities the installation wizard performed while transferring files.

Before you begin viewing log files, ensure that they contain the information that you need. The number of log files and the information they contain are set by parameters in IBM Cognos Connection and in IBM Cognos Configuration.

Use IBM Cognos Administration in IBM Cognos Connection to learn about logging categories and how to set the level of detail to log for each category.

For more information, see the IBM Cognos 8 *Administration and Security Guide*.

Use IBM Cognos Configuration to specify the size, number, and location of log files, and to configure the properties of the log server. For more information, see the IBM Cognos Configuration *User Guide*.

When troubleshooting, the following files can assist you:

The Transfer Log File

This file records the activities that the installation wizard performed while transferring files. The transfer log file is located in the `c8_location\instlog` directory. The file name identifies the product name, version, and build number, and includes a time stamp. The following is an example of the file name format:

`tl-C8BISRVR-8.1-0.0-20080901_1122.txt`

The Transfer Summary-Error Log File

This file records the components you installed, disk space information, the selections you made in the transfer dialogs, and any errors the installation wizard encountered while transferring components. The transfer summary-error log file is located in the *c8_location/instlog* directory. The file name identifies the product name, version, and build number, and includes a time stamp. The following is an example of the file name format:

tl-C8BISRV8-8.1-0.0-20080901_1122_summary_error.txt

The Startup Configuration File

This file records your configuration choices each time you save your property settings. The file name is *cogstartup.xml*. If you are unable to save your configuration, or are having problems you can revert to a previously saved configuration file. The backup configuration files are located in the *c8_location/configuration* directory. The following is an example of the file name format for backup configuration files:

cogstartup_200811231540.xml

The Startup Configuration Lock File

This file is created each time you open IBM Cognos Configuration. It prevents you from opening more than one IBM Cognos Configuration window. If you experience problems opening IBM Cognos Configuration, you can check the *c8_location/configuration* directory for the *cogstartup.lock* file. If the file exists and IBM Cognos Configuration is not open, it means that IBM Cognos Configuration did not shut down properly the last time you used it. You can delete the lock file and then open IBM Cognos Configuration.

The Locale Configuration File

This file records the configuration choices you make in IBM Cognos Configuration for product and content locales, locale mapping, and currency support. If you experience problems with language support in the user interface or in reports, use these files to track your changes. The backup configuration files are located in the *c8_location/configuration* directory. The following is an example of the file name format:

coglocale_200811231540.xml

The Run-Time Log File

The default IBM Cognos log file named *cogserver.log* file, or other log files that you configure to receive log messages from the log server, record information after you start the IBM Cognos 8 service. They are located in the *c8_location/logs* directory. If you configured another destination for log messages, check the appropriate file or database.

Some log messages indicate problems. Most messages provide information only, but others can help you to diagnose problems in your run-time environment.

The Gateway Log File

The gateways record errors in the gateway log file, which is located in the *c8_location/logs* directory. You can use the gateway log file to troubleshoot problems that prevent the gateway from processing requests or from using encryption. Symptoms of these problems are user IDs and passwords do not

work, single signon does not work, and the dispatcher is running but users receive the following error message: `The IBM Cognos BI server is not available`. The gateway log file uses the following naming format, where *gateway_interface* is `cgi`, `mod` (Apache 1.3 module), `mod2` (Apache 2.0 module), or `isapi`.

`gateway_interface.log` (e.g., `gwcgi.log`)

The Uninstallation Log File

This file records the activities that the Uninstall wizard performed while uninstalling files. The log file is named `cognos_uninst_log.htm` and is located in the Temp directory. You can use the log file to troubleshoot problems related to uninstalling IBM Cognos 8 components.

The Silent Mode Log File

This file records the activities that IBM Cognos Configuration performed while running in silent mode. This log file is named `cogconfig_response.csv` and is located in the `c8_location/logs` directory.

The ReportNet^(R) to IBM Cognos 8 Upgrade File

This file contains a summary of the results of an upgrade from ReportNet to IBM Cognos 8. The log file is named `upgradeLog.xml` and is located in the `c8_location/logs` directory. The file is in xml format and references an xslt style sheet. You can double-click the file to have it appear in your browser.

Problems Starting IBM Cognos 8

You may encounter problems when you try

- to start the IBM Cognos 8 service
- to open the Welcome page for IBM Cognos Connection for the first time
- to start an application server, such as WebLogic or WebSphere

Symptoms	Solution
You do not see the splash screen for IBM Cognos Connection when you start IBM Cognos 8.	Check your Web server configuration.
The service starts but no tables are created in the content store database.	Check your content store configuration.
The service does not start.	Ensure that you wait a few moments before submitting a request.
The application server does not start.	Check the file permissions and directory names of the application server installation location.

Ensure that you use other software that is supported by IBM Cognos components. You can view an up-to-date list of environments, such as operating systems, patches, browsers, Web servers, directory servers, and database servers on the Cognos Software Services Web site (<http://support.cognos.com>).

CFG-ERR-0106 Error When Starting the IBM Cognos 8 Service in IBM Cognos Configuration

When you start the IBM Cognos 8 service, you may receive the following error message:

CFG-ERR-0106 Cognos Configuration received no response from the Cognos 8 service in the allotted time. Check that Cognos 8 service is available and properly configured.

There are two possible causes for this problem:

- The IBM Cognos 8 service needs more time to start.
- A standby Content Manager computer may be configured incorrectly.

The IBM Cognos 8 Service Needs More Time

By default, IBM Cognos Configuration checks the progress of the start request every half second for three minutes. If IBM Cognos Configuration does not receive a response within this time, the error message appears.

To avoid this error, you can change the amount of time that IBM Cognos Configuration waits to receive a response from the IBM Cognos 8 service. You do this by configuring the `ServiceWaitInterval` and `ServiceMaxTries` properties in the `c8_location/configuration/cogconfig.prefs` file.

The `ServiceWaitInterval` property represents the time interval, in milliseconds, at which IBM Cognos Configuration checks the progress of the start request. By default, its value is 500, which is equivalent to half a second.

The `ServiceMaxTries` property represents the number of times that IBM Cognos Configuration checks the progress of the start request. By default, its value is 360.

Content Manager Is Configured Incorrectly

If the error message appears on a standby Content Manager computer, the setting for storing the symmetric keys may be incorrect.

To avoid this problem, configure the standby Content Manager computer to store the symmetric keys locally.

Steps to Change the Wait Time

1. Using IBM Cognos Configuration, stop the IBM Cognos 8 service.
2. Open the `c8_location/configuration/cogconfig.prefs` file in an editor.

This file is created automatically the first time you open IBM Cognos Configuration.

3. Add the following code to the file:

`ServiceWaitInterval=number of milliseconds`

`ServiceMaxTries=number of times`

Tip: Add the numeric values that correspond to your configuration needs.

4. Save the file.
5. Using IBM Cognos Configuration, start the IBM Cognos 8 service.

Steps to Store Symmetric Keys Locally

1. On the standby Content Manager computer, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, under **CSK settings**, set **Store symmetric key locally** to **True**.
4. From the **File** menu, click **Save**.
5. From the **Actions** menu, click **Start**.

This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Unable to Start the IBM Cognos 8 Service Because the Port is Used by Another Process

You may not be able to start the IBM Cognos 8 service or process if one of the default ports is used by another process.

Tip: To view the current network TCP/IP network connections, use the netstat command.

Use IBM Cognos Configuration to change the default port that IBM Cognos 8 uses.

When you change the port used by the local dispatcher, you must change the value of the Dispatcher URI properties. Because the change affects all the URIs that are based on the local dispatcher, you must change the URIs of all local components. By default, local components contain localhost in the URI.

For example, if you install all components on one computer and you want to change the dispatcher port, replace 9300 in all dispatcher and Content Manager URIs with the new port number.

Steps to Change the Default Port

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click the appropriate group or component:
 - To access the port number in the dispatcher and Content Manager URIs, click **Environment**.
 - To access the port number for the local log server, under **Environment**, click **Logging**.
 - To access the shutdown port number, under **Environment**, click **IBM Cognos 8 service**, **IBM Cognos 8**.
 - To access the port number for the location of the applications.xml file used by Portal Services, under **Environment**, click **Portal Services**.

3. In the **Properties** window, click the **Value** box next to the property that you want to change.
4. Change the value from 9300 to the new value.
Ensure that you change the ports in all URIs that contain localhost:9300.
5. From the **File** menu, click **Save**.
6. From the **Action** menu, click **Start**.

IBM Cognos BI Server Not Available When Starting IBM Cognos 8

After you configure IBM Cognos components and start the IBM Cognos 8 services, when you open IBM Cognos Connection, the following error message may appear:

The Cognos Gateway is unable to connect to the Cognos BI server.

The server may be unavailable, or the gateway may not be correctly configured.

Check the IBM Cognos server log file for more information. By default, the cogserver.log file is located in the *c8_location/logs* directory. If you configured another destination for log messages, check the appropriate file or database.

Content Manager may not be able to connect to the content store if the content store is not configured properly. This may occur if

- the content store uses an unsupported character encoding
- the content store uses a database collation sequence that is case sensitive
- the configuration settings you specified in IBM Cognos Configuration are not valid

Unsupported Character Encoding

If the following messages appear in the log file, the database you created for the content store does not use a supported character encoding:

- For Oracle:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

CM-SYS-5126 The content store database server uses the character set US7ASCII.

CM-SYS-5125 The content store database client uses the character set US7ASCII.

- For DB2 UDB:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

CM-SYS-5124 The content store database server uses the code page 1252.

- For Sybase:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

For Content Manager to connect to the content store, the content store must use the appropriate character encoding.

Database	Character encoding
Oracle 9i	AL32UTF8
	AL32UTF16
DB2 UDB	Codeset UTF-8
Sybase ASE	UTF-8
Microsoft SQL Server	UTF8
	UTF16

To resolve this problem, you must recreate the content store database using the correct character encoding, or convert the character encoding. For more information, see the database documentation.

Case Sensitive Collation Sequence

If the following messages appear in the log file, the database you created for the content store uses a database collation sequence that is case sensitive:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5122 The content store database has a default collation that is case-sensitive. Content Manager requires a content store that has a case-insensitive collation.

CM-SYS-5123 The content store database server uses the collation <parameter>.

CM-SYS-5007 Content Manager build @cm_build_version@ failed to start! Review the Content Manager log files and then contact your system administrator or customer support.

To resolve this problem, you must recreate the content store database using a database collation sequence that is not case sensitive. For more information, see the database documentation.

Invalid Configuration Settings

If the following or similar messages appear in the log file, you did not configure the content store correctly in IBM Cognos Configuration.

- For Microsoft SQL Server:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:SQLConnect://localhost:1433/cm".

Failed Logon:com.jnetdirect.jsql.x: Cannot open database requested in login 'cm'. Login fails. url:jdbc:SQLConnect://localhost:1433/cm.

- For DB2:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5003 Content Manager is unable to access the content store. Verify your database connection parameters and then contact your database administrator.

[IBM][CLI Driver] SQL1013N The database alias name or database name "CM123" could not be found.

- For Oracle:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:oracle:thin:@localhost:1521:pb1".

ORA-01017: invalid username/password; logon denied.

- For Sybase:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:sybase:Tds:localhost:5000/cm".

JZ006: Caught IOException: java.net.ConnectException: Connection refused: connect.

If you are using an Oracle database, do not use illegal characters such as an underscore in IBM Cognos Configuration for the Service Name property. If the Service Name includes illegal characters, tables are not created in the content store database when the IBM Cognos 8 service is started.

Steps for Microsoft SQL Server, Oracle, DB2, and Sybase

1. On the computer where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access, Content Manager**, right-click **Content Store** and click **Delete**.

This deletes the default resource. Content Manager must be configured to access only one content store.

3. Right-click **Content Manager**, and then click **New resource, Database**.
4. In the **Name** box, type a name for the resource.

5. In the **Type** box, select the type of database and click **OK**.

Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

6. In the **Properties** window, provide values depending on your database type:

- If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type `localhost\instance1`. If no instance name property is specified, a connection to the default instance is created.

Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

```
jdbc:SQLConnect://localhost\instance1/user=sa/more properties as required
```

- If you use a DB2 database, for the **Database name** property, type the database alias.
- If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.
- If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an example:

```
(description=(address=(host=myhost)(protocol=tcp)(port=1521)(connect_data=(sid=(orcl))))))
```

- If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.

7. If you want to change the logon credentials, specify a user ID and password:

- Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
- Type the appropriate values and click **OK**.

8. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

9. Test the connection between Content Manager and the content store.

Tip: In the **Explorer** window, right-click the new database and click **Test**.

Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Cannot Log On to a Namespace When Using IBM Cognos Connection (PRS-CSE-1255 Error)

You open IBM Cognos 8 through IBM Cognos Connection. However, when you attempt to create a data source and log on to a namespace, the following error messages appear:

- *PRS-CSE-1255 Exception error encountered in data decryption.*
- *CAM-CRP-1064 Unable to process the PKCS #7 data because of an internal error. Reason: java.lang.IndexOutOfBoundsException.*

This issue may occur if you do not have the necessary permissions for the following directories:

- c8\configuration
- c8\configuration\csk
- c8\configuration\encryptkeypair
- c8\configuration\signkeypair

The solution is to enable the read and execute permissions on the directories listed above for anyone who must start the IBM Cognos 8 service.

IBM Cognos 8 Services Fail to Restart After a Network Outage

The IBM Cognos Bootstrap Service restarts IBM Cognos 8 services after a network outage for Tomcat installations where a network IP address is specified in the internal dispatcher URI. During the restart, the IBM Cognos 8 services may not initialize successfully, requiring a manual restart after the network is restored.

To resolve the problem, configure the **Internal dispatcher URI** property in IBM Cognos Configuration to use localhost or the network host name.

No Warning That Installing a Later Version of IBM Cognos 8 Will Automatically Update the Earlier Version of the Content Store

You have a version of ReportNet installed on your computer. You install a later version into a new location. You use the same database for the content store for both versions. After you configure the later version and start the IBM Cognos 8 service, the earlier version of ReportNet no longer works because all content is automatically upgraded.

If you want to use different versions of ReportNet and IBM Cognos 8 after you upgrade, ensure that before you install the later version, you

- back up the database you use for the content store
- restore the backup to a new location

Alternatively, you can choose to use the deployment tool to import the entire content store from an earlier version to the later version. All existing content in the content store database is replaced by the imported content. You receive a warning message about this.

Content Manager Error When Starting IBM Cognos 8

After starting IBM Cognos 8, no BIBUSTKSERVMA process is started. There are errors listed in the pogo*****.log and cogserver.log files. Users receive errors in the browser when connecting to IBM Cognos Connection.

In the pogo*****.log file, an error related to Content Manager appears.

In the cogserver.log file, the following error appears:

An attempt to register the dispatcher in Content Manager was unsuccessful. Will retry periodically.

When connecting to `http://computer name/cognos8`, the following error messages appear in the browser:

- *DPR-ERR-2058 The dispatcher cannot service the request at this time. The dispatcher is still initializing*
- *SoapSocketException: Connection Refused*

IBM Cognos Configuration uses a user ID to bind to the LDAP database. If this user ID is moved to another group, IBM Cognos Configuration can no longer locate it.

To correct the problem, move the user ID back to the original group.

The Page Cannot Be Found When Starting IBM Cognos 8 in Windows 2003

After installing IBM Cognos 8 on Windows 2003, the following message may appear when you try to start IBM Cognos 8:

The page cannot be found. The page you are looking for might have been removed, had its name changed, or is temporarily unavailable. HTTP Error 404 - File or Directory not found.

This error is caused by a security feature in Windows 2003 Internet Information Services (IIS). This security feature does not allow unknown cgi file extensions.

To resolve this problem, add a new file extension in IIS for the cognos.cgi file. For more information, see the IIS documentation.

The Page Is Not Shown When Opening a Portal After Installing IBM Cognos 8

After you install and configure IBM Cognos 8, you are unable to open IBM Cognos Connection.

This may be because the Web server is not properly configured. For example, the virtual directories required for IBM Cognos 8 may not exist or they may point to the wrong physical folders.

For information about configuring the Web server, see the *Installation and Configuration Guide*.

DPR-ERR-2058 Error Appears in Web Browser When Starting IBM Cognos 8

After you start the services in IBM Cognos Configuration and then try to open the portal, a message similar to one of the following may appear:

DPR-ERR-2058 The dispatcher encountered an error while servicing a request. XTS handler must be initialized before being invoked.

DPR-ERR-2058 The dispatcher cannot service the request at this time. The dispatcher is still initializing. Please try again or contact your administrator.

These error messages usually occur when the dispatcher cannot communicate with Content Manager. To help you determine the specific cause, look in the `cogserver.log` file in the `c8_location/logs` directory. The most common causes are listed below, with solutions.

IBM Cognos Services are Not Done Initializing

After you start the services in IBM Cognos Configuration and the configuration tool shows that the services are running, wait a few minutes for all services to start before you open the portal.

Content Manager is Not Available

In a distributed installation, ensure that Content Manager is installed, configured, and running. Ensure also that the other IBM Cognos computers are configured with the correct Content Manager URI.

The Content Store is Not Available or is Not Configured Properly

Ensure that the content store database was created and that you configured it correctly in IBM Cognos Configuration.

Tables are Not Created in the Content Store

Ensure that you are using a version of DB2, Microsoft SQL Server, Oracle, or Sybase that is supported by IBM Cognos components.

The Logon Credentials for the Content Store Are Incorrect

Check whether the information changed. For example, DB2 reads information from the NT user management. If the password for the NT account changed, you must also change the logon credentials for the content store in IBM Cognos Configuration.

Check for special characters in the logon password. Occasionally, the JDBC driver does not accept characters that are reserved for xml, such as %, !, <, and >.

The User Does not Have Appropriate Permissions

Ensure that the user has the appropriate permissions.

Content Manager Cannot Connect to the Content Store on Oracle

If you are using an Oracle database as a content store, the DPR-ERR-2058 error may be generated when logging onto the portal `http://host_name/cognos8`. All tables are created on the database.

You may also receive the following error messages:

- *CM-CFG-5036 Content Manager failed to connect to the content store.*
- *ORA-01017: invalid username/password; logon denied*

Steps to Set the Oracle Database Server Name

1. In the Explorer window, click Data Access, Content Manager, Content Store.

2. Change the Oracle database server name to a fully qualified name such as `host_name.company-name:1534` to match the name in the `tnsnames.ora` file.

DPR-ERR-2022 Error Appears in Web Browser When Starting IBM Cognos 8

After you start the services in IBM Cognos Configuration and then try to open the portal, a message similar to the following may appear:

DPR-ERR-2022 No response generated. This may be due to an incorrect configuration, a damaged installation, or the dispatcher not having finished initializing.

Opening the Portal Too Soon

This problem can occur if you try to open the portal before IBM Cognos services are initialized.

To avoid this problem, after you start the services in IBM Cognos Configuration and the configuration tool shows that the services are running, wait a few minutes for all services to start before you open the portal.

The system.xml File Contains Errors

The `system.xml` file may have been edited.

Replace the `system.xml` file in the `c8_location\templates\ps\portal` directory with a copy from backup or use an XML editor to edit it.

Application Server Startup Script Fails

You may have problems running the startup scripts for an application server to deploy the IBM Cognos application if IBM Cognos 8 components are installed in a directory with a name that includes spaces.

To resolve this problem, rename the directory and do not include spaces in the new name. If this solution is not easily handled by the startup scripts, try adding quotation marks around the directory name that includes spaces or use the 8.3 DOS naming convention.

Permission Problems Using Contributor Administration or Analyst

You are using Contributor Administration or Analyst and receive errors indicating that you do not have the correct permissions when you perform such tasks as creating an application, adding user rights, or using Go To Production.

This can occur if you are using fully qualified domain names (FQDN) in the gateway URI in IBM Cognos Configuration for your Planning Administration clients and you are using a Microsoft Internet Information Services (IIS) 6.0 Web server and have Integrated Windows authentication enabled.

For example, if you have configured your Planning Administration client computer to use a gateway values such as

`http://servername.domain.com/cognos8/cgi-bin/cognos.cgi`

you may see these errors.

You can resolve this problem by using only the server name in the gateway URI value on your Planning Administration client computers, rather than the fully qualified domain name. For example, you can change your gateway URI value to something like

`http://servername/cognos8/cgi-bin/cognos.cgi`

If you have configured your Planning Server components to use the fully qualified domain name, you must install the Planning Administration clients on a different computer, and ensure that you use only the server name for the gateway, rather than the fully qualified domain name.

Problems Integrating IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning

If you are using IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning in an integrated environment, you may encounter problems.

Page Not Found Error When Trying to Open Analysis Studio

You have IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning installed on separate computers sharing the same content store. You try to open Analysis Studio from the IBM Cognos 8 Planning gateway and a Page Not Found error message appears.

To avoid this problem, install the gateway components of both IBM Cognos products into both the install location of IBM Cognos 8 Business Intelligence and the install location of IBM Cognos 8 Planning.

Failed to Load the Pluggable Shared Library When Using Analysis Studio

You have IBM Cognos 8 Business Intelligence and IBM Cognos 8 Planning installed on separate computers sharing the same content store. You open Analysis Studio from the IBM Cognos 8 Planning gateway and select a package that was created from a Contributor application. The following error message appears:

`Failed to load the pluggable shared library.`

To avoid this problem, start IBM Cognos Configuration on the planning server computer, disable the batch report service and the report service, then restart the IBM Cognos 8 and planning services.

Problems Using Contributor Administrator Caused by Incorrect Database Configuration

If a database client is not installed or configured correctly, an administrator may encounter problems when using Contributor Administration.

Problems Creating an Application in an SQL Environment

When using Contributor Administration to create an application in an SQL Environment, the following error message appears:

```
Unable to connect to computername using
SQL
Server Data Manipulation Objects (SQLDMO).
Unable to create the object with ProgID 'SQLDMO.SQLServer'
```

To avoid this problem, install Microsoft SQL Server on the computer where the planning server is installed.

Problems Creating an Application in a DB2 Environment

When using Contributor Administration to create an application using a DB2 datastore, the following error message appears:

```
Unable to execute the statement.~~~~The SQL was:~~CREATE
TABLE

The row length of the table exceeded a limit of "4005"
bytes.
```

To fix this problem, configure the DB2 tablespace size to be 8k instead of 4k.

Problems Importing Data in an SQL Environment

When using Contributor Administration to import data, the following error messages appear:

```
There was a problem during the load.
The error details have been recorded in the error log.
Unable to Bulk Load the data.
```

To avoid this problem, install Microsoft SQL Server on the computer where the planning server is installed.

Problems Running Go to Production in an SQL Environment

When using Contributor Administration to run the Go to Production process, the process fails and following error message appears in the log file:

```
Unable to execute the statement.Could not find database
ID 22. Database may not be activated yet or may be in transition.
```

To avoid this problem, install Microsoft SQL Server on the computer where the planning server is installed.

Problems Creating a Module in Framework Manager Using a SAP BW Data Source

If you set access permissions incorrectly to model and run reports using SAP BW as a data source, run time error messages may appear.

The BAP-ERR-0002 BAPI Error

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

BAP-ERR-0002 BAPI error occurred in function module BAPI_MDDATASET_CHECK_SYNTAX. Error occurred when starting the parser.

This error usually occurs because the SAP BW server is overloaded.

To resolve this problem, restart the IBM Cognos 8 server or close all open connections from the SAP BW Administrator Workbench.

The BAP-ERR-0002 BAPI Authorization Error for Function Group RSOB

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

BAP-ERR-0002 BAPI error occurred in function module BAPI_MDPROVIDER_GET_KEY_DATE. User COGNOS has no RFC authorization for function group RSOB.

To resolve this problem, provide the user COGNOS access to the function group RSOB.

The BAP-ERR-0002 BAPI Authorization Error for RFC_READ_TABLE

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

*BAP-ERR-0002 BAPI error occurred in function module RFC_READ_TABLE.
NOT_AUTHORIZED.*

This error occurs because displaying or editing table content is not authorized.

To resolve this problem, add the authorization object S_TABU_DIS with the activity field value set to DISPLAY and the Authorization Group value set to SS.

Authorization Error for Component

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

*<Message Name="CCLMessage" Severity="Error" Nesting="0">. <MessageParm
Name="CCLMessageParm" Type="string" Value="You do not have authorization for component
IDES_APO_PUMP_1"/>.*

This error occurs because access to infoqueries is not authorized.

To resolve this problem, provide access to S_RS_COMP and S_RS_COMP1.

Authorization Error for InfoCube

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

*<Message Name="CCLMessage" Severity="Error" Nesting="0">. <MessageParm
Name="CCLMessageParm" Type="string" Value="You do not have authorization for InfoCube
OAPO_C02"/>.*

This error occurs because access to infocubes is not authorized.

To resolve this problem, provide access to S_RS_ICUBE.

Authorization Error for Hierarchy

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

*SBW-ERR-0020 Querying the SAP BW cubes's failed. SAP error code: BAP-ERR-002 A BAPI
error has occurred in the function module BAPI_MDDATASET_GET_AXIS_DATA. No author-
ization for evaluation along hierarchy 01011.*

This error occurs because access to the infocube hierarchy is not authorized.

To resolve this problem, provide access to S_RS_HIER.

Authorization Error for Temporary File

When performing a Detailed Fact Query that contains a large number of items, the following error message may appear:

RQP-DEF-0177 An error occurred while performing operation 'sqlScrollBulkFetch' status='-232'. UDA-SQL-0107 A general exception has occurred during the operation "No authorization to open the file /tmp/ES1DEV03000807584_C.TMP.SYSTEM_FAILURE". UDA-CUR-0000 Unable to fetch the row.

This error occurs because access to temporary files is not authorized.

To resolve this problem, provide access to S_DATASET.

Authorization Errors Using the IBM Cognos SAP Gateway

If you install and configure IBM Cognos SAP gateway functions incorrectly, authorization error messages may appear.

Unable to Identify SAP Permissions Required

You may encounter errors using SAP BW because your SAP user signon does not have sufficient permissions. To identify the permissions needed, use the ST01 transaction.

Steps

1. In SAP R/3, type /ST01 in the command window.
2. Under **Trace components**, select **Authorization check**.
3. Select **Change trace**.
4. In the **Options for Trace Analysis Field**, under **General Restrictions**, enter the user name of the IBM Cognos account you are tracing.

Unable to Identify SAP BW Version and Corrections

You must use supported versions and patch levels of SAP BW, so you must be able to see a list of patches (correction notes) that have been applied. For more information about supported versions, see the Cognos Software Services website (<http://support.cognos.com>). To see a list of correction notes that have been applied, you can run one of two transactions in R/3: SE95, or SNOTE. In all cases, you must be authorized to run these transactions. In some cases, you may need to run the transactions using the same account that was used to apply the correction notes.

Steps

1. In SAP R/3, type /SE95 in the command window.
2. Enter an asterisk (*) in the Last Changed By field, to view all notes.
3. Select the type of modification in the Modifications tab.

Error Messages in SAP Log When Using Data Manager Connector for SAP R/3

You are using Data Manager Connector for SAP R/3 and the following error message appears in the SAP log:

DATASET_CANT_CLOSE

To resolve this problem, on computers where you have Data Manager components installed, create a system level environment variable named SAPCOMPRESSION and set the value to OFF.

Fact Table Does Not Include Any Data

When using IBM Cognos 8 with an SAP BW data source, the following error message may appear:

BMT-MD-5076 The fact table exists in the database but it does not contain any data. This may happen because this is a multi-provider cube.

This error can occur if you do not have udacompr.exe zlib1.dll on windows or LIBZ on UNIX installed in the SAP server RUN directory.

To resolve this problem, in the SAP server RUN directory, install udacompr.exe and zlib1.dll (on Windows) or LIBZ (on UNIX).

Glossary

access permissions

Rules defining the access rights to resources. Access permissions can be granted to any combination of namespaces, groups, or users. Examples of resources are reports and folders.

access tables

In Contributor, controls access to cells in cubes, whole cubes, and assumption cubes.

administration machine

In IBM Cognos Planning, the computer that is used to operate the Contributor Administration Console.

administration server

In IBM Cognos Planning, the server that contains the planning components package (COM+ package) and where control of the online application is maintained. You connect to this machine when you first run the Contributor Administration Console.

alias

In modeling and database terminology, a secondary name for a database table. Aliases are used to create a distinct reference to the table in the model, so that self-joins can be created or ambiguous query paths can be resolved.

In map information technology, a secondary name for a map feature. Aliases are used to create a reference between custom map feature names and feature names in databases.

anonymous access

A method of accessing resources in which users are not authenticated, and all users gain the same access permissions.

application

In IBM Cognos Planning, a Contributor application. Contributor applications are used for the collection and review of data from hundreds, or thousands of Web servers. One application can be used by many users in different locations at the same time.

Application server

See Job Server.

application tier components

For installation, the processors that access the query databases to gather information and then render the results as PDF and HTML reports and metrics. Application tier components also pass requests to Content Manager and render the results that Content Manager retrieves from the content store.

authentication

The process of verifying the identity of users when they log on. Users must be authenticated before they can be authorized to use any secured resources.

authentication provider

The communication mechanism to an external authentication source. Functionality such as user authentication, group membership, and namespace searches are made available through authentication providers.

certificate

A document that identifies someone or something by name. Certificates are issued by certification authorities. Each IBM Cognos computer in a distributed installation uses a different certificate. Certificates are used to positively identify an entity. They are used for digital signatures and secure communications, and can be used for encryption or decryption.

certification authority

Certification authority (CA) is the IBM Cognos component that issues certificates identification to each computer on which components are installed. You can also use other (non-IBM Cognos) certificate authorities.

cipher suite

In SSL, a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite to use when transmitting messages back and forth.

common gateway interface

(CGI) A standard that describes how Web servers should access other programs to create a document that will appear in a Web browser. For example, Web servers often use CGI programs to process forms.

connection

The named information that defines the type of the data source, its physical location, and any signon requirements. A data source can have more than one connection.

content locale

A code that is used to set the language or dialect used for browsers, report text, and so on; and the regional preferences, such as formats for time, date, money, money expressions, and time of day.

For IBM Cognos products, you can specify a locale for the product interface (product locale) and for the data in the report (content locale).

Content Manager

The IBM Cognos 8 service that manages the storage of customer applications, including application-specific security, configuration data, models, metrics, reports, and report output. Content Manager

is needed to publish models, retrieve or store report specifications, manage scheduling information, and manage the IBM Cognos namespace.

content store

The database that contains data that IBM Cognos 8 needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace, and the IBM Cognos namespace itself; and information about scheduling and bursting reports.

Design models and log files are not stored in the content store.

The IBM Cognos 8 service that uses the content store is named Content Manager.

Contributor Administration Console

A tool which enables administrators to publish an Analyst business model to the Web, manage access settings and model distribution, and configure the user's view of the model.

credentials

Information stored about the identity of an IBM Cognos user, usually a user name and password. You can assign your credentials to someone else so that they can use resources that you are authorized to use.

Credentials are created for IBM Cognos components. If a user schedules or programs an action, credentials must be stored in the content store.

data source

A relational database, dimensional cube, file, or other physical data store that can be accessed through IBM Cognos 8.

e.List

The basis for the structure of a Contributor application. An e.List is a hierarchical dimension which typically reflects the structure of the organization (for example, cost centers and profit centers).

extensions

In IBM Cognos Planning, extends the functionality of the Contributor Administration Console and Classic Web Client. There are two types of extensions: Admin Extensions and Client Extensions. Admin Extensions run in the Administration Console. Client Extensions are activated from the tool options on the Classic Contributor Grid.

gateway

An extension of a Web server program that transfers information from the Web server to another server. Gateways are often CGI programs, but may follow other standards such as ISAPI and Apache Modules.

go to production

In IBM Cognos Planning, a process in the Contributor Administration Console that takes the development application and creates the live production application.

group

In security, a list of users or other groups that can be used to assign access permissions and capabilities.

Groups can be referenced from other authentication sources or can be local to IBM Cognos 8. Local groups are managed from the administration portal. The list of groups that an authentication user is a member of is part of the user's passport for an IBM Cognos 8 session.

In reporting, grouping is the action of organizing common values of query item together and only displaying the value once. Headers and footers often appear after each instance of a common value in a grouped column

HTTPS

A secure version of HTTP Hypertext Transfer Protocol that incorporates secure sockets layer (SSL).

IBM Cognos products use HTTPS and SSL to encrypt and transmit passwords securely over the Internet.

job

A group of runnable objects, such as reports, agents, and other jobs that you run and schedule as a batch.

job server

In IBM Cognos Planning, a machine that runs the administration jobs. There may be multiple job servers. A job server is sometimes referred to as an application server.

job step

The smallest part of a job that can be run separately. Usually, a job step is a report. A job step can also be another job.

locale

A code that is used to set the language or dialect used for browsers, report text, and so on; and the regional preferences, such as formats for time, date, money, and money expressions.

For IBM Cognos products, you can specify a locale for the product interface (product locale) and for the data in the report (content locale).

maximum workspace

(MAXWS) The amount of memory reserved for Analyst. May be changed to allow larger models to run more effectively.

namespace

For authentication and access control, a configured instance of an authentication provider. Allows access to user and group information.

In XML, a collection of names, identified by a URI reference, which are used in XML documents as element types and attribute names.

In Framework Manager, namespaces uniquely identify query items, query subjects, and so on. You import different databases into separate namespaces to avoid duplicate names.

passport

Session-based information regarding authenticated users. A passport is created the first time a user accesses IBM Cognos 8. It is retained until a session ends, either when the user logs off, or after a specified period of inactivity.

Passport information is stored in Content Manager memory. Credentials are stored encrypted.

A passport is stored in a memory-only browser cookie for the duration of the session.

portlet

A mechanism for displaying Web content as part of a portal page.

product locale

The code or setting that specifies what language, regional settings, or both to use for parts of the product interface, such as menu commands.

publish

In IBM Cognos 8 BI, refers to exposing all or part of a Framework Manager model or Transformer PowerCube, via a package, to the IBM Cognos 8 server, so that it can be used to create reports and other content.

In IBM Cognos Planning, refers to a function that is used to copy the data from Contributor or Analyst to a datastore, typically so it can be used for reporting purposes.

publish container

In IBM Cognos Planning, a datastore container created specifically to publish data to.

security provider

See authentication provider.

user

A person accessing an IBM Cognos 8 application. User information, such as the location of personal folders or preferred formats for viewing reports, is stored in IBM Cognos 8.

Authenticated user definitions and information, such as passwords and IDs, are maintained in other authentication sources.

Index

Symbols

.xml configuration files, [39](#)

A

access

enabling authentication, [148](#)

access permissions

definition, [241](#)

access tables

definition, [241](#)

Active Directory Server

advanced properties, [152](#)

authenticating in multiple domains, [152](#)

enabling single signon, [153](#)

enabling SSL, [151](#)

using for authentication, [149](#)

with an LDAP namespace, [162](#)

active scripting

enabling in Web browsers, [50](#)

administration, [40](#)

IBM Cognos Connection, [40](#)

administration components

default settings, [102](#)

installing, [101](#)

administration machines

definition, [241](#)

administration servers

definition, [241](#)

agent service, [94](#)

aliases

configuring on Apache Web Server, [135](#)

configuring on Web servers, [78, 98](#)

definition, [241](#)

Analysis Studio problems, [236](#)

Analyst

accessing IBM Cognos 8 Planning outside a fire-wall, [103](#)

configuring, [103](#)

configuring on different computer, [103](#)

anonymous access

definition, [241](#)

anonymous logon

disabling, [148](#)

apache_mod file

configuring for gateways, [103, 114](#)

Apache gateways

configuring, [135](#)

Apache Web servers

configuring aliases, [78, 98](#)

configuring as gateways, [135](#)

applications

definition, [241](#)

application servers

startup script fails, [235](#)

application tier components

definition, [241](#)

authentication

Active Directory Server, [149](#)

configuring IBM Cognos Series 7 namespace, [154](#)

custom authentication providers, [158, 159](#)

custom properties for Active Directory Server, [150](#)

custom user properties for LDAP, [171](#)

definition, [241](#)

deleting namespaces, [182](#)

disabling anonymous logon, [148](#)

domain trees for Active Directory Server, [152](#)

enabling, [148](#)

eTrust Siteminder, [174, 176, 177](#)

LDAP, [160, 161](#)

LDAP using Active Directory Server, [162](#)

LDAP using IBM Directory Server, [165](#)

LDAP using Novell Directory Server, [167](#)

LDAP using Sun Java System Directory Server, [169](#)

NTLM, [178](#)

requirements for single signon with Microsoft Analysis Server or Microsoft SQL Server, [149](#)

SaferAPIGetTrustedSignon function, [156](#)

SAP, [179](#)

single signon for NTLM, [179](#)

single signon using Active Directory Server, [153](#)

- single signon using eTrust SiteMinder, [177](#)
- single signon using IBM Cognos Series 7
 - namespace, [155](#)
- single signon using LDAP, [173](#)
- single signon using SAP, [181](#)
- SSL for eTrust Siteminder, [177](#)
- SSL using LDAP, [172](#)
- testing namespaces, [182](#)
- trusted signon plug-ins for IBM Cognos Series 7, [156](#)
- using namespaces, [147](#)

authentication provider

- configuring IBM Cognos 8 to use security, [77](#), [87](#)

authentication providers

- definition, [242](#)

B

- BAP-ERR-0002 error, [238](#), [239](#), [240](#)

- BAP-ERR-0002 errors, [237](#)

- batch report service, [94](#)

- best practices, [9](#)

- Bind user DN and password property

- special characters for LDAP namespace, [160](#)

C

- CA, *See* [certification authority](#)

certificate authority

- configuring, [140](#)

certificates

- definition, [242](#)

certificate signing requests

- generating, [140](#)

certification authority

- configuring the service, [140](#)

- definition, [242](#)

changing

- configuration template, [127](#)

- default configuration settings, [119](#)

- IBM Cognos 8 gateway, [135](#)

- URIs, [120](#)

characters

- encoding not supported, [228](#)

- chase_referral files, [152](#)

cipher suites

- definition, [242](#)

- setting a priority for SSL connections, [133](#)

- Classic Contributor Web Client, [109](#)

client components

- installing, [109](#)

- code pages for data sources, [52](#)

- coglocale.xml files, [39](#)

- Cognos Software Services Web site, [11](#)

- cogstartup.lock file, [224](#)

- cogstartup.xml files, [39](#)

collation sequences

- case-sensitive, [228](#)

common gateway interface

- replacing, [135](#)

common gateway interface (CGI)

- definition, [242](#)

- common symmetric key, [122](#)

components

- Composite Information Server, [18](#)

- Content Manager, [18](#), [88](#)

- content store, [19](#)

- Event Studio, [18](#)

- Framework Manager, [19](#)

- gateways, [18](#), [88](#)

- IBM Cognos 8, [21](#)

- IBM Cognos Configuration, [18](#)

- IBM Cognos Connection, [17](#)

- IBM Cognos Viewer, [18](#)

- installing, [21](#), [88](#)

- planning store, [19](#)

- report server, [88](#)

- startup configuration, [38](#)

- used by IBM Cognos 8 Planning, [17](#)

Composite Information Server

- component description, [18](#)

- Confidentiality algorithm, [123](#)

configuration

- automating, [205](#)

- changing defaults settings, [119](#)

- changing the template, [127](#)

- default settings, [119](#)

- lock file, [224](#)

- requirements for single signon with Microsoft Analysis Server or Microsoft SQL Server, [149](#)

- security, [39](#)

- settings for IBM Cognos 8, [119](#)

- startup, [38](#)

- unable to open IBM Cognos Configuration, [224](#)

- unattended, [205](#), [208](#)

- workflows, [37](#)
- configuration files, [39](#)
 - applications.xml for Portal Services, [193](#)
 - exporting, [208](#)
- configuring
 - Active Directory namespace, [149](#)
 - Analyst, [103](#)
 - Analyst on different computer, [103](#)
 - apache_mod for the gateway, [103](#), [114](#)
 - certificate authority service, [140](#)
 - custom authentication providers, [159](#)
 - eTrust SiteMinder namespace, [176](#)
 - Framework Manager on different computer, [114](#)
 - IBM Cognos 8 Planning, [119](#)
 - IBM Cognos 8 service, [127](#)
 - IBM Cognos 8 to work with other IBM Cognos products, [139](#)
 - ISAPI for the gateway, [103](#), [114](#)
 - JDBC drivers, [49](#)
 - LDAP namespace, [161](#)
 - LDAP namespace for Active Directory Server, [162](#)
 - LDAP namespace for IBM Directory Server, [165](#)
 - NTLM namespace, [178](#)
 - Portal Services, [193](#)
 - routers, [52](#)
 - SAP namespace, [181](#)
 - servlets for the gateway, [103](#), [114](#)
 - shared trust with other servers, [132](#)
 - SSL protocol, [129](#)
 - standby Content Manager, [76](#), [86](#)
 - transfer specification files (.ats), [205](#)
 - unattended, [208](#)
 - Web browsers, [50](#)
 - Web server, [78](#), [98](#)
- connections
 - definition, [242](#)
- content locale
 - definition, [242](#)
- Content Manager
 - an attempt to register the dispatcher, [233](#)
 - component description, [18](#)
 - configuring on multiple computers, [76](#), [86](#)
 - definition, [242](#)
 - installing, [25](#), [88](#)
 - requirements if using IBM Cognos 8 Transformer with Series 7 namespace, [154](#)
 - setting up a content store, [44](#)
- Content Manager service, [94](#)
- Content Manager URIs, [76](#), [86](#)
- content store
 - component description, [19](#)
 - connection management, [73](#), [84](#)
 - creating, [44](#), [71](#), [81](#), [101](#)
 - DB2, [47](#)
 - definition, [243](#)
 - deploying, [62](#)
 - invalid settings, [228](#)
 - JDBC drivers, [49](#)
 - Microsoft SQL Server, [45](#)
 - Oracle, [46](#)
 - setting up database clients, [49](#)
 - Sybase Adaptive Server Enterprise, [48](#)
 - upgrading, [232](#)
- Contributor Administration Console
 - definition, [243](#)
- Contributor Administration problems, [236](#)
- Contributor for Microsoft Excel
 - installing, [110](#)
- Contributor Web Client, [106](#)
 - Classic Contributor Web Client, [13](#), [106](#)
 - CognosRCP.msi installation, [109](#)
 - Command line installation, [108](#)
 - contributor.msi installation, [109](#)
 - Contributor Administrator Console installation options, [107](#)
 - Installing, [106](#)
 - uninstall, [110](#)
 - Web link installation, [107](#)
- cookies
 - enabling in Web browsers, [50](#)
- copyright material
 - printing, [11](#)
- creating
 - content store, [71](#), [81](#), [101](#)
- credentials
 - definition, [243](#)
- cross-script checking
 - configuring in IBM Cognos Application Firewall, [124](#)
- cryptographic keys
 - generating for other certificate authorities, [140](#)
- custom authentication providers, [158](#)

- custom user properties
 - Active Directory Server, [150](#)
 - LDAP, [171](#)

D

- data
 - IBM Cognos samples, [211](#)
 - importing, [63](#)
- database client
 - setting up, [49](#)
- database connections
 - planning store, [75, 90](#)
- database connections, *See* [data source connections](#)
- database connection strings
 - IBM DB2, [73, 75, 84, 90](#)
 - Microsoft SQL Server, [73, 75, 84, 90](#)
 - Oracle, [73, 75, 84, 90](#)
- database connectivity
 - content store, [43](#)
- database drivers
 - OleDb, [44](#)
- databases
 - content store, [44](#)
 - IBM Cognos samples, [211](#)
 - planning store, [44](#)
- data integration service, [94](#)
- dataset errors
 - troubleshooting, [240](#)
- data source connections
 - setting, [73, 84](#)
- data sources
 - accessing SAP BW, [185](#)
 - definition, [243](#)
- DB2
 - code pages, [52](#)
 - content store, [47](#)
 - database connectivity, [43, 44](#)
 - environment variables, [47](#)
 - JDBC drivers, [49](#)
- DB2 content store, [145](#)
- default settings
 - administration components, [102](#)
- delivery service, [94](#)
- deploying
 - content store, [62](#)
 - exporting, [62](#)

- importing, [63](#)
- moving archives, [63](#)
- testing, [65](#)
- deployment
 - permissions, [61](#)
 - planning, [61](#)
- deployment archives
 - moving, [63](#)
- deployments
 - creating an export specification, [62](#)
- directory not found error, [233](#)
- distributed installation
 - large environment, [29](#)
 - medium environment, [29](#)
 - small environment, [28](#)
- distributed installations
 - configuring Analyst, [103](#)
 - configuring Framework Manager, [114](#)
- domains
 - Active Directory Server domain trees, [152](#)

E

- e.Lists
 - definition, [243](#)
- enabling
 - IBM Cognos Application Firewall, [124](#)
 - services, [126](#)
- environments
 - supported, [41](#)
- environment variables
 - content store, [44](#)
 - DB2, [47](#)
 - for Oracle data source, [112](#)
 - Oracle, [46](#)
- error messages
 - BAP-ERR-0002, [237, 238, 239, 240](#)
 - BAPI-MDDATASET_CHECK_SYNTAX, [237, 238, 239, 240](#)
 - CAM-CRP-1064, [232](#)
 - CFG-ERR-0106 Cognos Configuration received no response, [226](#)
 - DPR-ERR-2022 No response generated, [235](#)
 - DPR-ERR-2058, [233](#)
 - HTTP Error 404, [233](#)
 - page not found, [233](#)
 - PRS-CSE-1255, [232](#)

- SoapSocketException, [233](#)
- eTrust SiteMinder
 - configuring namespaces, [176](#)
 - cross-script checking in IBM Cognos Application Firewall, [124](#)
 - enabling single signon, [177](#)
 - protecting the IBM Cognos 8 Web alias, [177](#)
 - SSL, [177](#)
 - using for authentication, [174](#)
- event management service, [94](#)
- Event Studio
 - component description, [18](#)
- exporting
 - configuration files, [208](#)
 - creating a specification, [62](#)
- extensions
 - definition, [243](#)
- external identity mapping property
 - editing for an LDAP namespace, [174](#)
- External identity mapping property
 - special characters for LDAP namespace, [160](#)

F

- files
 - not found, [233](#)
- finding
 - information, [10](#)
- Firefox
 - browser settings, [50](#)
- firewalls
 - access between Analyst and IBM Cognos 8 Planning servers, [103](#)
 - access between Framework Manager and IBM Cognos 8, [114](#)
 - Framework Manager installation, [32](#)
- Framework Manager
 - accessing IBM Cognos 8 outside a firewall, [114](#)
 - component description, [19](#)
 - configuration requirements, [32](#)
 - configuring on different computer, [114](#)
 - configuring source control systems, [115](#)
 - installation options, [32](#)
 - installing, [111](#)
 - setting up the database client, [49](#)
 - system requirements, [112](#)
 - uninstalling, [78, 99, 117](#)

G

- gateway
 - log file, [224](#)
- gateways
 - component description, [18](#)
 - configuring apache_mod, [103, 114](#)
 - configuring a servlet, [103, 114](#)
 - configuring for IBM Cognos 8, [135](#)
 - configuring ISAPI, [103, 114](#)
 - configuring to use a namespace, [126](#)
 - definition, [243](#)
 - IBM Cognos 8, [23](#)
 - installing, [23, 88](#)
 - using on UNIX, [138](#)
- go to production
 - definition, [243](#)
- Great Outdoors
 - samples, [211](#)
- groups
 - definition, [243](#)

H

- help
 - getting, [11](#)
- histories
 - deployment, [65](#)
- HTTP Error 404, [233](#)
- HTTPS
 - definition, [244](#)

I

- IBM Cognos 8
 - configuring, [38](#)
 - default settings, [71, 81, 101](#)
 - dispatchers, [94](#)
 - installing, [37, 88](#)
 - logging in, [77, 87](#)
 - services, [94](#)
 - system requirements, [42](#)
 - troubleshooting installations, [223](#)
 - uninstalling, [78, 99](#)
- IBM Cognos 8 Business Intelligence
 - installing with IBM Cognos 8 Planning, [34](#)
- IBM Cognos8 Planning
 - server components, [17](#)

- IBM Cognos 8 Planning
 - components, [17](#)
 - configuring, [119](#)
 - modeling components, [18](#)
 - third-party components, [19](#)
 - IBM Cognos 8 service
 - configuring, [127](#)
 - requirements for the user account that is used for the service, [73](#), [84](#), [90](#), [97](#), [119](#)
 - server not available, [228](#)
 - IBM Cognos 8 Transformer
 - setting up the database client, [49](#)
 - IBM Cognos Application Firewall
 - configuring, [124](#)
 - IBM Cognos Configuration, [38](#)
 - component description, [18](#)
 - invalid settings, [228](#)
 - problems opening, [224](#)
 - unattended mode, [208](#)
 - IBM Cognos Connection
 - component description, [17](#)
 - unable to open, [233](#)
 - IBM Cognos namespace, [39](#)
 - IBM Cognos Series 7
 - enabling single signon, [155](#)
 - enabling SSL, [155](#)
 - trusted signon plug-ins, [156](#)
 - using for authentication, [154](#)
 - IBM Cognos Viewer
 - component description, [18](#)
 - IBM DB2
 - creating connection strings, [73](#), [75](#), [84](#), [90](#)
 - IBM Directory Server
 - with an LDAP namespace, [165](#)
 - IIS Web servers
 - single signon using Active Directory, [153](#)
 - implementation preparation, [37](#)
 - importing
 - data into target environment, [63](#)
 - InfoCubes
 - accessing using OLAP, [185](#)
 - information
 - finding, [10](#)
 - installation
 - checklist, [71](#), [81](#), [101](#)
 - components, [37](#)
 - Content Manager, [25](#)
 - Framework Manager, [32](#)
 - gateways, [23](#)
 - options, [21](#)
 - Planning Server, [25](#)
 - unattended, [205](#)
 - with IBM Cognos 8 Business Intelligence, [34](#)
 - workflows, [37](#)
 - installations
 - large environment, [29](#)
 - medium environment, [29](#)
 - small environment, [28](#)
 - installing
 - administration components, [101](#)
 - clients on Windows Vista, [109](#), [110](#)
 - Framework Manager, [111](#)
 - gateway functions for SAP BW, [185](#)
 - IBM Cognos 8, [71](#), [81](#), [88](#), [101](#), [205](#)
 - IBM Cognos 8 Planning client components, [109](#)
 - testing, [88](#), [99](#)
 - unattended, [38](#)
 - unattended install, [205](#)
 - using transfer specification file (.ats), [205](#)
 - using transfer specification files (.ats), [205](#)
 - Integrated Windows Authentication
 - configuring, [104](#)
 - Internet Explorer
 - browser settings, [50](#)
 - invalid settings
 - content store, [228](#)
 - IBM Cognos Configuration, [228](#)
 - ISAPI
 - accessing IBM Cognos 8, [135](#)
 - configuring for gateway, [103](#), [114](#)
- ## J
- Java scripts
 - enabling in Web browsers, [50](#)
 - Java System Web Server
 - configuring aliases, [78](#), [98](#)
 - JDBC, [49](#)
 - database connectivity for content store, [43](#)
 - DB2, [49](#)
 - Oracle databases, [50](#)
 - jobs
 - definition, [244](#)

- job servers
 - definition, [244](#)
- job service, [94](#)
- job steps
 - definition, [244](#)
- L**
- LDAP
 - Active Directory Server, [162](#)
 - configuring a namespace, [161](#)
 - custom properties, [171](#)
 - editing the External identity mapping property, [174](#)
 - enabling single signon, [173](#)
 - enabling SSL, [172](#)
 - IBM Directory Server, [165](#)
 - Novell Directory Server, [167](#)
 - Sun Java System Directory Server, [169](#)
 - using for authentication, [160](#)
- Linux
 - system requirements, [71](#), [81](#), [101](#)
 - unsupported features and components, [41](#)
- load balancing
 - enabling and disabling services, [126](#)
- locales
 - definition, [244](#)
- log files, [223](#)
 - for gateway errors, [224](#)
 - locale configuration, [224](#)
 - run-time, [224](#)
 - silent mode, [225](#)
 - startup configuration, [224](#)
 - transfer, [223](#)
 - transfer summary, [224](#)
 - uninstallation, [225](#)
- logging in
 - configuring security, [77](#), [87](#)
 - hiding namespaces during, [159](#), [177](#)
- log messages
 - enabling for IBM Cognos Application Firewall, [124](#)
- M**
- maximum workspace
 - definition, [244](#)
- Microsoft Analysis Server
 - namespace requirement, [149](#)
- Microsoft Analysis Services
 - setting up the data source environment, [52](#)
 - single signon to MSAS data sources, [153](#)
- Microsoft SQL Server
 - content store, [45](#)
 - creating connection strings, [73](#), [75](#), [84](#), [90](#)
 - database connectivity, [43](#), [44](#)
 - namespace requirement, [149](#)
- modeling components, [18](#)
- monitoring service, [94](#)
- moving
 - deployment archives, [63](#)
- Moving from trial upgrade to production environment, [65](#)
- MSAS, *See* [Microsoft Analysis Services](#)
- multi_domain_tree, [152](#)
- N**
- namespace
 - cannot log on, [232](#)
- namespaces
 - authentication, [147](#)
 - configuring custom authentication providers, [159](#)
 - configuring for a gateway, [126](#)
 - definition, [244](#)
 - deleting, [182](#)
 - hiding during login, [159](#), [177](#)
 - requirements for Content Manager if using Transformer with Series 7 namespace, [154](#)
 - testing, [182](#)
- Netegrity SiteMinder, *See* [eTrust SiteMinder](#)
- Netscape
 - browser settings, [50](#)
- network outage
 - services fail to start, [232](#)
- no response generated, [235](#)
- Novell Directory Server
 - with an LDAP namespace, [167](#)
- NTLM, [178](#)
 - configuring, [178](#)
 - enabling single signon, [179](#)
- NTLM, *See Also* [Windows native security \(NTLM\)](#)
- O**
- OLAP
 - accessing SAP BW, [185](#)

OLEDB

database drivers, [44](#)

Oracle

content store, [46](#)

creating connections strings, [73](#), [75](#), [84](#), [90](#)

database connectivity, [43](#), [44](#)

environment variables, [46](#)

environment variables for data source, [112](#)

JDBC drivers, [50](#)

multilingual support, [52](#)

P

page not found error

starting IBM Cognos 8 in Windows 2003, [233](#)

page not found error in Analysis Studio, [236](#)

passports

definition, [245](#)

performance

BAPI error, [238](#), [239](#), [240](#)

BAPI errors, [237](#)

permissions

deployment, [61](#)

for the user account that is used for the IBM Cognos
8 service, [73](#), [84](#), [90](#), [97](#), [119](#)

planning administration components

installing, [101](#)

planning an upgrade, [57](#)

planning client components

installing, [109](#)

planning data service, [95](#)

planning job service, [95](#)

Planning Server

installing, [25](#)

planning store

component description, [19](#)

creating, [44](#)

setting connection properties, [75](#), [90](#)

planning Web service, [95](#)

planning administration console service, [95](#)

pluggable shared library not loaded, [236](#)

portal

errors in starting, [233](#), [235](#)

portal problems

unable to open, [233](#)

Portal Services, [193](#)

availability on Linux, [41](#)

specifying the applications.xml file, [193](#)

portlets

definition, [245](#)

ports

changing, [120](#)

ports already in use, [227](#)

preparation

implementation, [37](#)

presentation service, [94](#)

printing copyright material, [11](#)

problems creating an application, [236](#), [237](#)

problems opening IBM Cognos Configuration, [224](#)

problems running Go to Production, [237](#)

product locale

definition, [245](#)

publish containers

definition, [245](#)

publishing

definition, [245](#)

Q

quality of protection in SSL connections, [133](#)

quick tours

using, [11](#)

R

readme

reviewing before you install, [41](#)

related documentation, [10](#)

ReportNet

to IBM Cognos 8 upgrade file, [225](#)

reports

testing before an upgrade, [60](#)

report servers

installing, [88](#)

report services, [95](#)

response.ats file, [205](#)

reviewing the readme before you install, [41](#)

routers

configuring, [52](#)

S

SaferAPIGetTrustedSignon function

using for authentication, [156](#)

samples

setting up, [211](#)

- SAP
 - enabling single signon, 181
 - using for authentication, 179
- SAP BW
 - accessing as a data source, 185
 - accessing using OLAP, 185
 - authorization settings for IBM Cognos 8 administrators, 181
 - authorization settings for IBM Cognos 8 users, 179
 - connectivity, 181
 - unable to identify SAP permissions, 239
 - unable to identify version, 239
 - using as a data source, 185
- secure LDAP communication, 172
- Secure Sockets Layer, *See* [SSL protocol](#)
- security
 - configuration, 39
 - enabling, 77, 87
 - settings for Web browsers, 42
- security providers
 - definition, 245
- server components, 17
- services
 - agent, 94
 - batch report, 94
 - Content Manager, 94
 - data integration, 94
 - delivery, 94
 - enabling and disabling, 126
 - event management, 94
 - fail to start after network outage, 232
 - IBM Cognos 8, 94
 - job, 94
 - monitoring, 94
 - planning data, 95
 - presentation, 94
 - report, 95
 - unable to start, 227
 - uninstalling, 78, 99
- setting
 - data source connections, 73, 84
- setting up
 - samples, 211
- shared trust
 - setting up between IBM Cognos 8 and other servers, 132
- silent configurations, 205
- silent installations, 205
- silent mode, 205
- single signon
 - Active Directory namespace, 153
 - eTrust SiteMinder user directory, 177
 - LDAP namespace, 173
 - NTLM namespace, 179
 - SAP namespace, 181
 - using IBM Cognos Series 7 namespace, 155
- source control systems
 - configuring for Framework Manager, 115
- special characters
 - in LDAP namespace properties, 160
- SQL Server databases
 - creating content store, 45
- SSL
 - Active Directory Server, 151
 - enabling on Web servers, 128, 133
 - eTrust SiteMinder user directory, 177
 - LDAP namespace, 172
 - quality of protection, 133
 - setting up shared trust with other servers, 132
 - using IBM Cognos Series 7 namespace, 155
- SSL protocol
 - configuring, 129
- standby Content Manager
 - configuring, 76, 86
- startup
 - configuration lock file, 224
 - page not found, 233
 - problems, 225
 - script fails, 235
 - unable to open IBM Cognos Connection, 233
 - unable to start service, 227
- startup configuration, 38
 - files, 39
- Sun Java System Directory Server
 - with an LDAP namespace, 169
- supported environments, 41
- Sybase
 - database drivers, 50
- Sybase Adaptive Server Enterprise
 - content store, 48
- system requirements, 42
 - Framework Manager, 112

T

tablespaces, [145](#)

template

changing the size of template, [127](#)

testing

deployment, [65](#)

testing the installation, [88, 99](#)

third-party components, [19](#)

transfer specification files (.ats)

configuration, [205](#)

Transformer

requirements for Content Manager if using Series 7

namespace, [154](#)

trial upgrade, [60](#)

planning the move to the production environment, [65](#)

troubleshooting, [223](#)

Contributor Administration problems, [236](#)

creating an application, [236, 237](#)

dataset errors, [240](#)

importing data, [237](#)

running Go to Production, [237](#)

troubleshooting Analysis Studio, [236](#)

tuning

DB2 content store, [145](#)

U

UDB, *See* [DB2](#)

unable to open IBM Cognos Configuration, [224](#)

unattended configuration

setting up, [205](#)

unattended installation, [38](#)

setting up, [205](#)

unattended mode, [205](#)

uninstalling

Framework Manager, [78, 99, 117](#)

IBM Cognos 8, [78, 99, 117](#)

UNIX

environment variables for Oracle data source, [112](#)

system requirements, [71, 81, 101](#)

UNIX gateway, [138](#)

unsupported characters, [228](#)

upgrading

content store, [232](#)

create test environment, [60](#)

from Planning, [55](#)

planning the move from test to production environment, [65](#)

preparation, [57](#)

process, [55](#)

resources, [59](#)

URI

changing, [120](#)

User account

requirements to run the IBM Cognos 8 service, [73, 84, 90, 97, 119](#)

User lookup property

special characters for LDAP namespace, [160](#)

users

definition, [245](#)

V

virtual directories

IBM Cognos 8, [78, 98](#)

W

Web aliases

IBM Cognos 8, [78, 98](#)

Web browsers

configuring, [50](#)

errors in starting the Web portal, [235](#)

errors when starting the web portal, [233](#)

security settings, [42](#)

WebLogic

startup script fails, [235](#)

Web servers, [32](#)

configuring, [78, 98](#)

enabling SSL, [128, 133](#)

single signon using Active Directory and IIS Web server, [153](#)

WebSphere Application Server

startup script fails, [235](#)

Windows

system requirements, [71, 81, 101](#)

Windows integrated authentication, [153](#)

Windows native security (NTLM)

enabling single signon, [179](#)

using for authentication, [178](#)

Windows Vista

installing clients on, [109, 110](#)

workflows

installation and configuration, [37](#)

X

XML configuration files, [39](#)